DoD CHIEF INFORMATION OFFICER
--
LAWS, REGULATIONS, AND POLICIES

2009 Edition

Table of Contents

Foreword

The Department's approach to the management of information technology (IT) and information-related activities is rooted in Federal laws and regulations that have evolved over the last three decades. This booklet, first published in 2000 and popularly known as "The Purple Book," is a collection of these laws and regulations, tracing *how* and *why* they came to be.

Originating in the 1977 recommendations of the Commission on Federal Paperwork, the IRM[1] approach was first enacted into law in the Paperwork Reduction Act of 1980 (PRA, Title 44 United States Code 3501 and sequence). The 1980 Act gave the Office of Management and Budget (OMB) specific policy-setting and oversight duties regarding individual IRM areas[2]; and it gave agencies a more general responsibility to carry out their IRM activities in an efficient, effective, and economical manner and to comply with OMB policies and guidelines. To assist in this effort, the law required that each agency head designate a senior IRM official who would report directly to the agency head to carry out the responsibilities of the agency under the law. Together these requirements were intended to provide for a coordinated approach to managing Federal agencies' information resources.

Amendments to the PRA in 1986 and in 1995 were designed to strengthen agency and OMB implementation of the law. For example, the PRA of 1995 provided detailed agency requirements for each IRM area, to match specific OMB provisions. The 1995 Act also required agencies to develop for the first time, processes to select, control, and evaluate the results of major information systems initiatives. Notwithstanding PRA, the world was rapidly changing and IT management problems in the government persisted, leading to widespread consensus in Congress and the Administration that meaningful IT management reform was needed.

---

[1] Information Resources Management (IRM) means the process of managing information and related resources, such as personnel, equipment, funds, and information technology.

[2] IRM areas include information management, records management, privacy, security, and IT acquisition.

Led by Senator William Cohen, Congress enacted the Information Technology Management Reform Act of 1996 – later combined with the Federal Acquisition Reform Act (FARA) and renamed the Clinger-Cohen Act of 1996 (now known as Title 40 USC Subtitle III). Supplementing the IT provisions of the PRA, the 1996 Act emphasized up-front capital planning and the establishment of clear performance goals and investment criteria designed to improve agency operations. The thinking was that once the up-front planning was completed and the performance goals were established, the procurement reforms (e.g., FARA) that Congress had enacted earlier would make it simpler and faster for agencies to purchase IT.

In addition, the 1996 Act establishes the position of Chief Information Officer (CIO) in major departments and agencies in the Federal government by amending the PRA to rename the Senior IRM Official, the CIO. It also requires the individual holding the position report directly to the agency head and have IRM as the "primary duty." The expectation was and continues to be that elevating the former IRM position to a more executive, strategic level would create a focus of leadership, responsibility and accountability for agencies' information management (IM) and IT activities and appreciably help to resolve persistent IT problems. Other Congressional expectations, including the duties of the Deputy CIO, can be found in House of Representatives (HR) Report 104-450: National Defense Authorization Act for Fiscal Year 1996 Conference Report.

The amendment to PRA includes a provision that the Secretary of the Department of Defense and the Secretaries of the Military Departments may each designate CIOs, stipulating that if more than one CIO is designated, the respective duties of the CIOs shall be clearly delineated. Accordingly, in a March 1996 memorandum[3], the Deputy Secretary of Defense designated the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I), now the ASD for Networks and Information Integration) as "the Chief Information Officer of the Department." The functions of the ASD (C3I) were substantially identical to those proposed for the agency CIO. In addition, the Deputy Secretary directed that "CIOs be established in each of the Military Departments and Defense Agencies."

[3] Deputy Secretary of Defense Memo, "Designation of the Chief Information Officer of the Department of Defense," dated March 14, 1996.

When Senator Cohen became Secretary of Defense, he issued a memorandum[4] that for several reasons is arguably the seminal document for implementing Title 40 in the Department. First, it clarifies that the Department has only one DoD CIO. Second, it delegates to the DoD CIO all the duties given to the Head of the Agency in the Act. Third, it clarifies the role of the DoD CIO vis-à-vis that of the DoD Component CIOs – DoD Component CIOs act as advisors to the DoD CIO, and implement the policies and guidance issued by the DoD CIO. Last, along with Title 10 of the United States Code, sections 2223 and 2224, it is the basis for:

- DoD Directive 5144.01, Assistant Secretary of Defense (Networks & Information Integration)/Department of Defense Chief Information Officer, dated May 5, 2005
- DoD Directive 8000.01, Management of the Department of Defense Information Enterprise, dated February 10, 2009

Other key laws and regulations, external and internal to DoD, continue to guide the Department of Defense Information Enterprise in this fast-paced, Information Age global environment. For example, the E-Government Act (44 USC 36) includes the Federal Information Security Management Act, OMB Circular A-130, the National and Defense Information Sharing Strategies, and DoD Information Assurance issuances. All serve as references as we design, build, operate and protect information solutions to gain and maintain the information advantage for DoD personnel and mission partners.

[4] Secretary of Defense Memo, Implementation of Division E of the Clinger-Cohen of 1996 (Public Law 104-106), dated June 7, 1997.

44 United States Code 3501 et seq.

Also known as Paperwork Reduction Act	
Public Law	104-13, 109-435, 110-289
Date	May 22, 1995, updated as of January 2, 2006
Reports	U.S. House. Committee on Government Reform. H. Report No. 104-37 U.S. Senate. Committee on Governmental Affairs. S. Report No. 104-8 U.S. House. Conference Report. H. Report No. 104-99

An Act to further the goals of the Paperwork Reduction Act to have Federal agencies become more responsible and publicly accountable for reducing the burden of Federal paperwork on the public, and for other purposes.

Short Title. This Act may be cited as the "Paperwork Reduction Act of 1995".

Sec. 2. Coordination of Federal Information Policy.

Chapter 35 of title 44, United States Code, is amended to read as follows:

CHAPTER 35 -- COORDINATION OF FEDERAL INFORMATION POLICY

Sec. 3501. Purposes

The purposes of this chapter are to –

(1) minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government;

(2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government;

(3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public;

(4) improve the quality and use of Federal information to strengthen decision-making, accountability, and openness in Government and society;

(5) minimize the cost to the Federal Government of the creation, collection, maintenance, use, dissemination, and disposition of information;

(6) strengthen the partnership between the Federal Government and State, local, and tribal governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government;

(7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology;

(8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to

(A) privacy and confidentiality, including section 552a of title 5;

(B) security of information, including the Computer Security Act of 1987 (Public Law 100-235); and

(C) access to information, including section 552 of title 5;

(9) ensure the integrity, quality, and utility of the Federal statistical system;

(10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public; and

(11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this subchapter.

Sec. 3502. Definitions

As used in this chapter –

(1) the term "agency" means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include –

(A) the General Accounting Office;

(B) Federal Election Commission;

(C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or

(D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities;

(2) the term "burden" means time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for –

(A) reviewing instructions;

(B) acquiring, installing, and utilizing technology and systems;

(C) adjusting the existing ways to comply with any previously applicable instructions and requirements;

(D) searching data sources;

(E) completing and reviewing the collection of information; and

(F) transmitting, or otherwise disclosing the information;

(3) the term "collection of information" –

(A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either --

(i) answers to identical questions posed to, or identical reporting or record-keeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(B) shall not include a collection of information described under section 3518(c)(1);

(4) the term "Director" means the Director of the Office of Management and Budget;

(5) the term "independent regulatory agency" means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Rela-

tions Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission;

(6) the term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology;

(7) the term "information resources management" means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public;

(8) the term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

(9) the term "information technology" has the meaning given that term in section 11101 of title 40 but does not include national security systems as defined in section 11103 of title 40;

(10) the term "person" means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(11) the term "practical utility" means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion;

(12) the term "public information" means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public;

(13) the term "recordkeeping requirement" means a requirement imposed by or for an agency on persons to maintain specified records, including a requirement to --

(A) retain such records;

(B) notify third parties, the Federal Government, or the public of the existence of such records;

(C) disclose such records to third parties, the Federal Government, or the public; or

(D) report to third parties, the Federal Government, or the public regarding such records; and

(14) the term "penalty" includes the imposition by an agency or court of a fine or other punishment; a judgment for monetary damages or equitable relief; or the revocation, suspension, reduction, or denial of a license, privilege, right, grant, or benefit.

Sec. 3503. Office of Information and Regulatory Affairs

(a) There is established in the Office of Management and Budget an office to be known as the Office of Information and Regulatory Affairs.

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall delegate to the Administrator the authority to administer all functions under this subchapter, except that any such delegation shall not relieve the Director of responsibility for the administration of such functions. The Administrator shall serve as principal adviser to the Director on Federal information resources management policy.

Sec. 3504. Authority and Functions of Director

(a)(1) The Director shall oversee the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions, including burden reduction and service delivery to the public. In performing such oversight, the Director shall --

(A) develop, coordinate and oversee the implementation of Federal information resources management policies, principles, standards, and guidelines; and

(B) provide direction and oversee –

(i) the review and approval of the collection of information and the reduction of the information collection burden;

(ii) agency dissemination of and public access to information;

(iii) statistical activities;

(iv) records management activities;

(v) privacy, confidentiality, security, disclosure, and sharing of information; and

(vi) the acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures.

(2) The authority of the Director under this chapter shall be exercised consistent with applicable law.

(b) With respect to general information resources management policy, the Director shall –

(1) develop and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines;

(2) foster greater sharing, dissemination, and access to public information, including through –

(A) the use of the Government Information Locator Service; and

(B) the development and utilization of common standards for information collection, storage, processing and communication, including standards for security, interconnectivity and interoperability;

(3) initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices;

(4) oversee the development and implementation of best practices in information resources management, including training; and

(5) oversee agency integration of program and management functions with information resources management functions.

(c) With respect to the collection of information and the control of paperwork, the Director shall --

(1) review and approve proposed agency collections of information;

(2) coordinate the review of the collection of information associated with Federal procurement and acquisition by the Office of Information and Regulatory Affairs with the Office of Federal Procurement Policy, with particular emphasis on applying information technology to improve the efficiency and effectiveness of Federal procurement, acquisition and payment, and to reduce information collection burdens on the public;

(3) minimize the Federal information collection burden, with particular emphasis on those individuals and entities most adversely affected;

(4) maximize the practical utility of and public benefit from information collected by or for the Federal Government;

(5) establish and oversee standards and guidelines by which agencies are to estimate the burden to comply with a proposed collection of information.

(6) publish in the Federal Register and make available on the Internet (in consultation with the Small Business Administration) on an annual basis a list of

the compliance assistance resources available to small businesses, with the first such publication occurring not later than 1 year after the date of enactment of the Small Business Paperwork Relief Act of 2002.

(d) With respect to information dissemination, the Director shall develop and oversee the implementation of policies, principles, standards, and guidelines to --

(1) apply to Federal agency dissemination of public information, regard-less of the form or format in which such information is disseminated; and

(2) promote public access to public information and fulfill the purposes of this chapter, including through the effective use of information technology.

(e) With respect to statistical policy and coordination, the director shall—

(1) coordinate the activities of the Federal statistical system to endure—

(A) the efficiency and effectiveness of the system; and

(B) the integrity, objectivity, impartiality, utility, and confidentiality of information collected for statistical purposes.

(2) ensure that budget proposals of agencies are consistent with system-wide priorities for maintaining and improving the quality of Federal statistics and prepare an annual report on statistical program funding;

(3) develop and oversee the implementation of Governmentwide policies, principles, standards, and guidelines concerning

(A) statistical collection procedures and methods;

(B) statistical data classification;

(C) statistical information presentation and dissemination

(D) timely release of statistical data; and

(E) such statistical data sources as may be required for the administration of Federal programs;

(4) evaluate statistical program performance and agency compliance with Governmentwide policies, principles, standards, and guidelines;

(5) promote the sharing of information collected for statistical purposes consistent with privacy rights and confidentiality pledges;

(6) coordinate the participation of the United States in international statistical activities, including the development of comparable statistics;

(7) appoint a chief statistician who is a trained and experienced professional statistician to carry out the functions described under this subsection

(8) establish an Interagency Council on Statistical policy to advise and assist the Director in carrying out the functions under this subsection that shall—

(A) be headed by the chief statistician; and

(B) consist of—

(i) the heads of the major statistical programs; and

(ii) the representatives of other statistical agencies under rotating membership; and

(9) provide opportunities for training in statistical policy functions to employees of the Federal Government under which—

(A) each trainee shall be selected at the discretion of the Director based on agency requests and shall service under the chief statistician for at least 6 months and not more than 1 year; and

(B) all costs of the training shall be paid by the agency requesting training.

(f) With respect to records management, the Director shall --

(1) provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination in the administration of chapters 29, 31, and 33 of this title with the information resources management policies, principles, standards, and guidelines established under this subchapter;

(2) review compliance by agencies with –

(A) the requirements of chapters 29, 31, and 33 of this title; and

(B) regulations promulgated by the Archivist of the United States and the Administrator of General Services; and

(3) oversee the application of records management policies, principles, standards, and guidelines, including requirements for archiving information maintained in electronic format, in the planning and design of information systems.

(g) With respect to privacy and security, the Director shall --

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and

(2) oversee and coordinate compliance with sections 552 and 552a of title 5, sections 20 and 21 of the National Institute of Standards and Technology Act

(15 U.S.C. 278g-3 and 278-4) section 11331 of title 40 and subchapter II of this chapter, and related information management laws.

(h) With respect to Federal information technology, the Director shall --

(1) in consultation with the Director of the National Institute of Standards and Technology and the Administrator of General Services --

(A) develop and oversee the implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government, including periodic evaluations of major information systems; and

(B) oversee the development and implementation of standards under section 11331 of title 40;

(2) monitor the effectiveness of, and compliance with, directives issued under subtitle III of title 40 and directives issued under section 322 of title 40;

(3) coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy;

(4) ensure, through the review of agency budget proposals, information resources management plans and other means –

(A) agency integration of information resources management plans, pro-gram plans and budgets for acquisition and use of information technology; and

(B) the efficiency and effectiveness of inter-agency information technology initiatives to improve agency performance and the accomplishment of agency missions; and

(5) promote the use of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of Federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

Sec. 3505. Assignment of Tasks and Deadlines

(a) In carrying out the functions under this subchapter, the Director shall

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to --

(A) reduce information collection burdens imposed on the public that

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506(c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

(2) with selected agencies and non-Federal entities on a voluntary basis, conduct pilot projects to test alternative policies, practices, regulations, and procedures to fulfill the purposes of this subchapter, particularly with regard to minimizing the Federal information collection burden; and

(3) in consultation with the Administrator of General Services, the Direc-tor of the National Institute of Standards and Technology, the Archivist of the United States, and the Director of the Office of Personnel Management, develop and maintain a Governmentwide strategic plan for information resources management, that shall include

(A) a description of the objectives and the means by which the Federal Government shall apply information resources to improve agency and program performance;

(B) plans for –

(i) reducing information burdens on the public, including reducing such burdens through the elimination of duplication and meeting shared data needs with shared resources;

(ii) enhancing public access to and dissemination of, information, using electronic and other formats; and

(iii) meeting the information technology needs of the Federal Government in accordance with the purposes of this chapter; and

(C) a description of progress in applying information resources management to improve agency performance and the accomplishment of missions.

(b) For purposes of any pilot project conducted under subsection (a)(2), the Director may, after consultation with the agency head, waive the application of any administrative directive issued by an agency with which the project is conducted, including any directive requiring a collection of information, after giving timely notice to the public and the Congress regarding the need for such waiver.

(c) Inventory of Major Information Systems. (1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

(3) Such inventory shall be—

(A) updated at least annually;

(B) made available to the Comptroller General; and

(C) used to the support information resources management, including—

(i) preparation and maintenance of the inventory of information resources under section 3506 (b) (4);

(ii) information technology planning, budgeting, acquisition, and management under section 3506 (h), subtitle III of title 40, and related laws and guidance;

(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

(iv) preparation of the index of major information systems required under section 552 (g) of title 5, United States Code; and

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.

(c) Inventory of Information Systems.—(1) The head of each agency shall develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency;

(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency;

(3) Such inventory shall be—

(A) updated at least annually;

(B) made available to the Comptroller General; and

(C) used to support information resources management, including—

(i) preparation and maintenance of the inventory of information resources under section 3506 (b)(4);

(ii) information technology planning, budgeting, acquisition, and management under section 3506 (h), subtitle III of title 40, and related laws and guidance;

(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

(iv) preparation of the index of major information systems required under section 552 (g) of title 5, United States Code; and

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.

Sec. 3506. Federal Agency Responsibilities

(a)(1) The head of each agency shall be responsible for—

(A) carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness; and

(B) complying with the requirements of this subchapter and related policies established by the Director.

(2)(A) Except as provided under subparagraph (B), the head of each agency shall designate a Chief Information Officer who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.

(B) The Secretary of the Department of Defense and the Secretary of each military department may each designate Chief Information Officers who shall report directly to such Secretary to carry out the responsibilities of the department under this subchapter. If more than one Chief Information Officer is designated, the respective duties of the Chief Information Officers shall be clearly delineated.

(3) The Chief Information Officer designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this subchapter, including the reduction of information collection burdens on the public. The Chief Information Officer and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this subchapter.

(4) Each agency program official shall be responsible and accountable for information resources assigned to and supporting the programs under such

official. In consultation with the Chief Information Officer designated under paragraph (2) and the agency Chief Financial Officer (or comparable official), each agency program official shall define program information needs and develop strategies, systems, and capabilities to meet those needs.

(b) With respect to general information resources management, each agency shall—

(1) manage information resources to—

(A) reduce information collection burdens on the public;

(B) increase program efficiency and effectiveness; and

(C) improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security;

(2) in accordance with guidance by the Director, develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions;

(3) develop and maintain an ongoing process to—

(A) ensure that information resources management operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions;

(B) in cooperation with the agency Chief Financial Officer (or comparable official), develop a full and accurate accounting of information technology expenditures, related expenses, and results; and

(C) establish goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness, methods for measuring progress towards those goals, and clear roles and responsibilities for achieving those goals;

(4) in consultation with the Director, the Administrator of General Services, and the Archivist of the United States, maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511 of this subchapter; and

(5) in consultation with the Director and the Director of the Office of Personnel Management, conduct formal training programs to educate agency program and management officials about information resources management.

(c) With respect to the collection of information and the control of paperwork, each agency shall—

(1) establish a process within the office headed by the Chief Information Officer designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this subchapter, to—

(A) review each collection of information before submission to the Director for review under this subchapter, including—

(i) an evaluation of the need for the collection of information;

(ii) a functional description of the information to be collected;

(iii) a plan for the collection of the information;

(iv) a specific, objectively supported estimate of burden;

(v) a test of the collection of information through a pilot program, if appropriate; and

(vi) a plan for the efficient and effective management and use of the information to be collected, including necessary resources;

(B) ensure that each information collection—

(i) is inventoried, displays a control number and, if appropriate, an expiration date;

(ii) indicates the collection is in accordance with the clearance requirements of section 3507; and

(iii) informs the person receiving the collection of information of—

(I) the reasons the information is being collected;

(II) the way such information is to be used;

(III) an estimate, to the extent practicable, of the burden of the collection;

(IV) whether responses to the collection of information are voluntary, required to obtain a benefit, or mandatory; and

(V) the fact that an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number; and

(C) assess the information collection burden of proposed legislation affecting the agency;

(2)(A) except as provided under subparagraph (B) or section 3507 (j), provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information, to solicit comment to—

(i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

(ii) evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;

(iii) enhance the quality, utility, and clarity of the information to be collected; and

(iv) minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology; and

(B) for any proposed collection of information contained in a proposed rule (to be reviewed by the Director under section 3507 (d)), provide notice and comment through the notice of proposed rulemaking for the proposed rule and such notice shall have the same purposes specified under subparagraph (A)(i) through (iv);

(3) certify (and provide a record supporting such certification, including public comments received by the agency) that each collection of information submitted to the Director for review under section 3507—

(A) is necessary for the proper performance of the functions of the agency, including that the information has practical utility;

(B) is not unnecessarily duplicative of information otherwise reasonably accessible to the agency;

(C) reduces to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency, including with respect to small entities, as defined under section 601 (6) of title 5, the use of such techniques as—

(i) establishing differing compliance or reporting requirements or time-tables that take into account the resources available to those who are to respond;

(ii) the clarification, consolidation, or simplification of compliance and reporting requirements; or

(iii) an exemption from coverage of the collection of information, or any part thereof;

(D) is written using plain, coherent, and unambiguous terminology and is understandable to those who are to respond;

(E) is to be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and recordkeeping practices of those who are to respond;

(F) indicates for each recordkeeping requirement the length of time persons are required to maintain the records specified;

(G) contains the statement required under paragraph (1)(B)(iii);

(H) has been developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected,

including the processing of the information in a manner which shall enhance, where appropriate, the utility of the information to agencies and the public;

(I) uses effective and efficient statistical survey methodology appropriate to the purpose for which the information is to be collected; and

(J) to the maximum extent practicable, uses information technology to reduce burden and improve data quality, agency efficiency and responsiveness to the public; and

(4) in addition to the requirements of this chapter regarding the reduction of information collection burdens for small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)), make efforts to further reduce the information collection burden for small business concerns with fewer than 25 employees.

(d) With respect to information dissemination, each agency shall—

(1) ensure that the public has timely and equitable access to the agency's public information, including ensuring such access through—

(A) encouraging a diversity of public and private sources for information based on government public information;

(B) in cases in which the agency provides public information maintained in electronic format, providing timely and equitable access to the underlying data (in whole or in part); and

(C) agency dissemination of public information in an efficient, effective, and economical manner;

(2) regularly solicit and consider public input on the agency's information dissemination activities;

(3) provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(4) not, except where specifically authorized by statute—

(A) establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public;

(B) restrict or regulate the use, resale, or redissemination of public information by the public;

(C) charge fees or royalties for resale or redissemination of public information; or

(D) establish user fees for public information that exceed the cost of dissemination.

(e) With respect to statistical policy and coordination, each agency shall—

(1) ensure the relevance, accuracy, timeliness, integrity, and objectivity of information collected or created for statistical purposes;

(2) inform respondents fully and accurately about the sponsors, purposes, and uses of statistical surveys and studies;

(3) protect respondents' privacy and ensure that disclosure policies fully honor pledges of confidentiality;

(4) observe Federal standards and practices for data collection, analysis, documentation, sharing, and dissemination of information;

(5) ensure the timely publication of the results of statistical surveys and studies, including information about the quality and limitations of the surveys and studies; and

(6) make data available to statistical agencies and readily accessible to the public.

(f) With respect to records management, each agency shall implement and enforce applicable policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

(g) With respect to privacy and security, each agency shall—

(1) implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency; and

(2) assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, subchapter II of this chapter, and related information management laws.

(h) With respect to Federal information technology, each agency shall—

(1) implement and enforce applicable Governmentwide and agency information technology management policies, principles, standards, and guidelines;

(2) assume responsibility and accountability for information technology investments;

(3) promote the use of information technology by the agency to improve the productivity, efficiency, and effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information;

(4) propose changes in legislation, regulations, and agency procedures to improve information technology practices, including changes that improve the ability of the agency to use technology to reduce burden; and

(5) assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives through a process that is—

(A) integrated with budget, financial, and program management decisions; and

(B) used to select, control, and evaluate the results of major information systems initiatives.

(i)(1) In addition to the requirements described in subsection (c), each agency shall, with respect to the collection of information and the control of paperwork, establish 1 point of contact in the agency to act as a liaison between the agency and small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(2) Each point of contact described under paragraph (1) shall be established not later than 1 year after the date of enactment of the Small Business Paperwork Relief Act of 2002.

Sec. 3507. Public Information Collection Activities; Submission to Director; Approval and Delegation

(a) An agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information—

(1) the agency has—

(A) conducted the review established under section 3506 (c)(1);

(B) evaluated the public comments received under section 3506 (c)(2);

(C) submitted to the Director the certification required under section 3506 (c)(3), the proposed collection of information, copies of pertinent statutory authority, regulations, and other related materials as the Director may specify; and

(D) published a notice in the Federal Register—

(i) stating that the agency has made such submission; and

(ii) setting forth—

(I) a title for the collection of information;

(II) a summary of the collection of information;

(III) a brief description of the need for the information and the proposed use of the information;

(IV) a description of the likely respondents and proposed frequency of response to the collection of information;

(V) an estimate of the burden that shall result from the collection of information; and

(VI) notice that comments may be submitted to the agency and Director;

(2) the Director has approved the proposed collection of information or approval has been inferred, under the provisions of this section; and

(3) the agency has obtained from the Director a control number to be displayed upon the collection of information.

(b) The Director shall provide at least 30 days for public comment prior to making a decision under subsection (c), (d), or (h), except as provided under subsection (j).

(c)(1) For any proposed collection of information not contained in a proposed rule, the Director shall notify the agency involved of the decision to approve or disapprove the proposed collection of information.

(2) The Director shall provide the notification under paragraph (1), within 60 days after receipt or publication of the notice under subsection (a)(1)(D), whichever is later.

(3) If the Director does not notify the agency of a denial or approval within the 60-day period described under paragraph (2)—

(A) the approval may be inferred;

(B) a control number shall be assigned without further delay; and

(C) the agency may collect the information for not more than 1 year.

(d)(1) For any proposed collection of information contained in a proposed rule—

(A) as soon as practicable, but no later than the date of publication of a notice of proposed rulemaking in the Federal Register, each agency shall forward to the Director a copy of any proposed rule which contains a collection of information and any information requested by the Director necessary to make the determination required under this subsection; and

(B) within 60 days after the notice of proposed rulemaking is published in the Federal Register, the Director may file public comments pursuant to the standards set forth in section 3508 on the collection of information contained in the proposed rule;

(2) When a final rule is published in the Federal Register, the agency shall explain—

(A) how any collection of information contained in the final rule responds to the comments, if any, filed by the Director or the public; or

(B) the reasons such comments were rejected.

(3) If the Director has received notice and failed to comment on an agency rule within 60 days after the notice of proposed rulemaking, the Director may not disapprove any collection of information specifically contained in an agency rule.

(4) No provision in this section shall be construed to prevent the Director, in the Director's discretion—

(A) from disapproving any collection of information which was not specifically required by an agency rule;

(B) from disapproving any collection of information contained in an agency rule, if the agency failed to comply with the requirements of paragraph (1) of this subsection;

(C) from disapproving any collection of information contained in a final agency rule, if the Director finds within 60 days after the publication of the final rule that the agency's response to the Director's comments filed under paragraph (2) of this subsection was unreasonable; or

(D) from disapproving any collection of information contained in a final rule, if—

(i) the Director determines that the agency has substantially modified in the final rule the collection of information contained in the proposed rule; and

(ii) the agency has not given the Director the information required under paragraph (1) with respect to the modified collection of information, at least 60 days before the issuance of the final rule.

(5) This subsection shall apply only when an agency publishes a notice of proposed rulemaking and requests public comments.

(6) The decision by the Director to approve or not act upon a collection of information contained in an agency rule shall not be subject to judicial review.

(e)(1) Any decision by the Director under subsection (c), (d), (h), or (j) to disapprove a collection of information, or to instruct the agency to make substantive or material change to a collection of information, shall be publicly available and include an explanation of the reasons for such decision.

(2) Any written communication between the Administrator of the Office of Information and Regulatory Affairs, or any employee of the Office of Information and Regulatory Affairs, and an agency or person not employed by the Federal Government concerning a proposed collection of information shall be made available to the public.

(3) This subsection shall not require the disclosure of—

(A) any information which is protected at all times by procedures established for information which has been specifically authorized under criteria estab-

lished by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(B) any communication relating to a collection of information which is not approved under this subchapter, the disclosure of which could lead to retaliation or discrimination against the communicator.

(f)(1) An independent regulatory agency which is administered by 2 or more members of a commission, board, or similar body, may by majority vote void—

(A) any disapproval by the Director, in whole or in part, of a proposed collection of information of that agency; or

(B) an exercise of authority under subsection (d) of section 3507 concerning that agency.

(2) The agency shall certify each vote to void such disapproval or exercise to the Director, and explain the reasons for such vote. The Director shall without further delay assign a control number to such collection of information, and such vote to void the disapproval or exercise shall be valid for a period of 3 years.

(g) The Director may not approve a collection of information for a period in excess of 3 years.

(h) (1) If an agency decides to seek extension of the Director's approval granted for a currently approved collection of information, the agency shall—

(A) conduct the review established under section 3506 (c), including the seeking of comment from the public on the continued need for, and burden imposed by the collection of information; and

(B) after having made a reasonable effort to seek public comment, but no later than 60 days before the expiration date of the control number assigned by the Director for the currently approved collection of information, submit the collection of information for review and approval under this section, which shall include an explanation of how the agency has used the information that it has collected.

(2) If under the provisions of this section, the Director disapproves a collection of information contained in an existing rule, or recommends or instructs the agency to make a substantive or material change to a collection of information contained in an existing rule, the Director shall—

(A) publish an explanation thereof in the Federal Register; and

(B) instruct the agency to undertake a rulemaking within a reasonable time limited to consideration of changes to the collection of information contained in the

rule and thereafter to submit the collection of information for approval or disapproval under this subchapter.

(3) An agency may not make a substantive or material modification to a collection of information after such collection has been approved by the Director, unless the modification has been submitted to the Director for review and approval under this subchapter.

(i)(1) If the Director finds that a senior official of an agency designated under section 3506 (a) is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved and has sufficient resources to carry out this responsibility effectively, the Director may, by rule in accordance with the notice and comment provisions of chapter 5 of title 5, United States Code, delegate to such official the authority to approve proposed collections of information in specific program areas, for specific purposes, or for all agency purposes.

(2) A delegation by the Director under this section shall not preclude the Director from reviewing individual collections of information if the Director determines that circumstances warrant such a review. The Director shall retain authority to revoke such delegations, both in general and with regard to any specific matter. In acting for the Director, any official to whom approval authority has been delegated under this section shall comply fully with the rules and regulations promulgated by the Director.

(j)(1) The agency head may request the Director to authorize a collection of information, if an agency head determines that—

(A) a collection of information—

(i) is needed prior to the expiration of time periods established under this subchapter; and

(ii) is essential to the mission of the agency; and

(B) the agency cannot reasonably comply with the provisions of this subchapter because—

(i) public harm is reasonably likely to result if normal clearance procedures are followed;

(ii) an unanticipated event has occurred; or

(iii) the use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information or is reasonably likely to cause a statutory or court ordered deadline to be missed.

(2) The Director shall approve or disapprove any such authorization request within the time requested by the agency head and, if approved, shall assign the collection of information a control number. Any collection of information conducted under this subsection may be conducted without compliance with the provisions of this subchapter for a maximum of 180 days after the date on which the Director received the request to authorize such collection.

Sec. 3508. Determination of Necessity for Information; Hearing

Before approving a proposed collection of information, the Director shall determine whether the collection of information by the agency is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility. Before making a determination the Director may give the agency and other interested persons an opportunity to be heard or to submit statements in writing. To the extent, if any, that the Director determines that the collection of information by an agency is unnecessary for any reason, the agency may not engage in the collection of information.

Sec. 3509. Designation of Central Collection Agency

The Director may designate a central collection agency to obtain information for two or more agencies if the Director determines that the needs of such agencies for information will be adequately served by a single collection agency, and such sharing of data is not inconsistent with applicable law. In such cases the Director shall prescribe (with reference to the collection of information) the duties and functions of the collection agency so designated and of the agencies for which it is to act as agent (including reimbursement for costs). While the designnation is in effect, an agency covered by the designation may not obtain for itself information for the agency which is the duty of the collection agency to obtain. The Director may modify the designation from time to time as circumstances require. The authority to designate under this section is subject to the provisions of section 3507(f) of this subchapter.

Sec. 3510. Cooperation of Agencies in Making Information Available

(a) The Director may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained by a collection of information if the disclosure is not inconsistent with applicable law.

(b)(1) If information obtained by an agency is released by that agency to another agency, all the provisions of law (including penalties) that relate to the unlawful disclosure of information apply to the officers and employees of the

agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

(2) The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

Sec. 3511. Establishment and Operation of Government Information Locator Service

(a) In order to assist agencies and the public in locating information and to promote information sharing and equitable access by the public, the Director shall—

(1) cause to be established and maintained a distributed agency-based electronic Government Information Locator Service (hereafter in this section referred to as the "Service"), which shall identify the major information systems, holdings, and dissemination products of each agency;

(2) require each agency to establish and maintain an agency information locator service as a component of, and to support the establishment and operation of the Service;

(3) in cooperation with the Archivist of the United States, the Administrator of General Services, the Public Printer, and the Librarian of Congress, establish an interagency committee to advise the Secretary of Commerce on the development of technical standards for the Service to ensure compatibility, promote information sharing, and uniform access by the public;

(4) consider public access and other user needs in the establishment and operation of the Service;

(5) ensure the security and integrity of the Service, including measures to ensure that only information which is intended to be disclosed to the public is disclosed through the Service; and

(6) periodically review the development and effectiveness of the Service and make recommendations for improvement, including other mechanisms for improving public access to Federal agency public information.

(b) This section shall not apply to operational files as defined by the Central Intelligence Agency Information Act (50 U.S.C. 431 et seq.).

Sec. 3512. Public Protection

(a) Notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information that is subject to this subchapter if—

(1) the collection of information does not display a valid control number assigned by the Director in accordance with this subchapter; or

(2) the agency fails to inform the person who is to respond to the collection of information that such person is not required to respond to the collection of information unless it displays a valid control number.

(b) The protection provided by this section may be raised in the form of a complete defense, bar, or otherwise at any time during the agency administrative process or judicial action applicable thereto.

Sec. 3513. Director Review of Agency Activities; Reporting; Agency Response

(a) In consultation with the Administrator of General Services, the Archivist of the United States, the Director of the National Institute of Standards and Technology, and the Director of the Office of Personnel Management, the Director shall periodically review selected agency information resources management activities to ascertain the efficiency and effectiveness of such activities to improve agency performance and the accomplishment of agency missions.

(b) Each agency having an activity reviewed under subsection (a) shall, within 60 days after receipt of a report on the review, provide a written plan to the Director describing steps (including milestones) to—

(1) be taken to address information resources management problems identified in the report; and

(2) improve agency performance and the accomplishment of agency missions.

Sec. 3514. Responsiveness to Congress

(a) (1) The Director shall—

(A) keep the Congress and congressional committees fully and currently informed of the major activities under this subchapter; and

(B) submit a report on such activities to the President of the Senate and the Speaker of the House of Representatives annually and at such other times as the Director determines necessary.

(2) The Director shall include in any such report a description of the extent to which agencies have—

(A) reduced information collection burdens on the public, including—

(i) a summary of accomplishments and planned initiatives to reduce collection of information burdens;

(ii) a list of all violations of this subchapter and of any rules, guidelines, policies, and procedures issued pursuant to this subchapter;

(iii) a list of any increase in the collection of information burden, including the authority for each such collection; and

(iv) a list of agencies that in the preceding year did not reduce information collection burdens in accordance with section 3505 (a)(1), a list of the programs and statutory responsibilities of those agencies that precluded that reduction, and recommendations to assist those agencies to reduce information collection burdens in accordance with that section;

(B) improved the quality and utility of statistical information;

(C) improved public access to Government information; and

(D) improved program performance and the accomplishment of agency missions through information resources management.

(b) The preparation of any report required by this section shall be based on performance results reported by the agencies and shall not increase the collection of information burden on persons outside the Federal Government.

Sec. 3515. Administrative Powers

Upon the request of the Director, each agency (other than an independent regulatory agency) shall, to the extent practicable, make its services, personnel, and facilities available to the Director for the performance of functions under this subchapter.

Sec. 3516. Rules and Regulations

The Director shall promulgate rules, regulations, or procedures necessary to exercise the authority provided by this subchapter.

Sec. 3517. Consultation with Other Agencies and the Public

(a) In developing information resources management policies, plans, rules, regulations, procedures, and guidelines and in reviewing collections of information, the Director shall provide interested agencies and persons early and meaningful opportunity to comment.

(b) Any person may request the Director to review any collection of information conducted by or for an agency to determine, if, under this subchapter, a person shall maintain, provide, or disclose the information to or for the agency. Unless the request is frivolous, the Director shall, in coordination with the agency responsible for the collection of information—

(1) respond to the request within 60 days after receiving the request, unless such period is extended by the Director to a specified date and the person making the request is given notice of such extension; and

(2) take appropriate remedial action, if necessary.

Sec. 3518. Effect on Existing Laws and Regulations

(a) Except as otherwise provided in this subchapter, the authority of an agency under any other law to prescribe policies, rules, regulations, and procedures for Federal information resources management activities is subject to the authority of the Director under this subchapter.

(b) Nothing in this subchapter shall be deemed to affect or reduce the authority of the Secretary of Commerce or the Director of the Office of Management and Budget pursuant to Reorganization Plan No. 1 of 1977 (as amended) and Executive order, relating to telecommunications and information policy, procurement and management of telecommunications and information systems, spectrum use, and related matters.

(c)(1) Except as provided in paragraph (2), this subchapter shall not apply to the collection of information—

(A) during the conduct of a Federal criminal investigation or prosecution, or during the disposition of a particular criminal matter;

(B) during the conduct of—

(i) a civil action to which the United States or any official or agency thereof is a party; or

(ii) an administrative action or investigation involving an agency against specific individuals or entities;

(C) by compulsory process pursuant to the Antitrust Civil Process Act and section 13 of the Federal Trade Commission Improvements Act of 1980; or

(D) during the conduct of intelligence activities as defined in section 3.4(e) of Executive Order No. 12333, issued December 4, 1981, or successor orders, or during the conduct of cryptologic activities that are communications security activities.

(2) This subchapter applies to the collection of information during the conduct of general investigations (other than information collected in an antitrust investtigation to the extent provided in subparagraph (C) of paragraph (1)) undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

(d) Nothing in this subchapter shall be interpreted as increasing or decreasing the authority conferred by sections 11331 and 11332 [1] of title 40 on the Secretary of Commerce or the Director of the Office of Management and Budget.

(e) Nothing in this subchapter shall be interpreted as increasing or decreasing the authority of the President, the Office of Management and Budget or the Director thereof, under the laws of the United States, with respect to the substantive policies and programs of departments, agencies and offices, including the substantive authority of any Federal agency to enforce the civil rights laws.

Sec. 3519. Access to Information

Under the conditions and procedures prescribed in section 716 of title 31, the Director and personnel in the Office of Information and Regulatory Affairs shall furnish such information as the Comptroller General may require for the discharge of the responsibilities of the Comptroller General. For the purpose of obtaining such information, the Comptroller General or representatives thereof shall have access to all books, documents, papers and records, regardless of form or format, of the Office.

Sec. 3520. Establishment of Task Force on Information Collection and Dissemination

(a) There is established a task force to study the feasibility of streamlining requirements with respect to small business concerns regarding collection of information and strengthening dissemination of information (in this section referred to as the "task force").

(b)(1) The Director shall determine—

(A) subject to the minimum requirements under paragraph (2), the number of representatives to be designated under each subparagraph of that paragraph; and

(B) the agencies to be represented under paragraph (2)(K).

(2) After all determinations are made under paragraph (1), the members of the task force shall be designated by the head of each applicable department or agency, and include—

(A) 1 representative of the Director, who shall convene and chair the task force;

(B) not less than 2 representatives of the Department of Labor, including 1 representative of the Bureau of Labor Statistics and 1 representative of the Occupational Safety and Health Administration;

(C) not less than 1 representative of the Environmental Protection Agency;

(D) not less than 1 representative of the Department of Transportation;

(E) not less than 1 representative of the Office of Advocacy of the Small Business Administration;

(F) not less than 1 representative of the Internal Revenue Service;

(G) not less than 2 representatives of the Department of Health and Human Services, including 1 representative of the Centers for Medicare and Medicaid Services;

(H) not less than 1 representative of the Department of Agriculture;

(I) not less than 1 representative of the Department of the Interior;

(J) not less than 1 representative of the General Services Administration; and

(K) not less than 1 representative of each of 2 agencies not represented by representatives described under subparagraphs (A) through (J).

(c) The task force shall—

(1) identify ways to integrate the collection of information across Federal agencies and programs and examine the feasibility and desirability of requiring each agency to consolidate requirements regarding collections of information with respect to small business concerns within and across agencies, without negatively impacting the effectiveness of underlying laws and regulations regarding such collections of information, in order that each small business concern may submit all information required by the agency—

(A) to 1 point of contact in the agency;

(B) in a single format, such as a single electronic reporting system, with respect to the agency; and

(C) with synchronized reporting for information submissions having the same frequency, such as synchronized quarterly, semiannual, and annual reporting dates;

(2) examine the feasibility and benefits to small businesses of publishing a list by the Director of the collections of information applicable to small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)), organized—

(A) by North American Industry Classification System code;

(B) by industrial sector description; or

(C) in another manner by which small business concerns can more easily identify requirements with which those small business concerns are expected to comply;

(3) examine the savings, including cost savings, and develop recommendations for implementing—

(A) systems for electronic submissions of information to the Federal Government; and

(B) interactive reporting systems, including components that provide immediate feedback to assure that data being submitted—

(i) meet requirements of format; and

(ii) are within the range of acceptable options for each data field;

(4) make recommendations to improve the electronic dissemination of information collected under Federal requirements;

(5) recommend a plan for the development of an interactive Government-wide system, available through the Internet, to allow each small business to—

(A) better understand which Federal requirements regarding collection of information (and, when possible, which other Federal regulatory requirements) apply to that particular business; and

(B) more easily comply with those Federal requirements; and

(6) in carrying out this section, consider opportunities for the coordination—

(A) of Federal and State reporting requirements; and

(B) among the points of contact described under section 3506 (i), such as to enable agencies to provide small business concerns with contacts for information collection requirements for other agencies.

(d) The task force shall—

(1) by publication in the Federal Register, provide notice and an opportunity for public comment on each report in draft form; and

(2) make provision in each report for the inclusion of—

(A) any additional or dissenting views of task force members; and

(B) a summary of significant public comments.

(e) Not later than 1 year after the date of enactment of the Small Business Paperwork Relief Act of 2002, the task force shall submit a report of its findings under subsection (c) (1), (2), and (3) to—

(1) the Director;

(2) the chairpersons and ranking minority members of—

(A) the Committee on Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate; and

(B) the Committee on Government Reform and the Committee on Small Business of the House of Representatives; and

(3) the Small Business and Agriculture Regulatory Enforcement Ombudsman designated under section 30(b) of the Small Business Act (15 U.S.C. 657 (b)).

(f) Not later than 2 years after the date of enactment of the Small Business Paperwork Relief Act of 2002, the task force shall submit a report of its findings under subsection (c) (4) and (5) to—

(1) the Director;

(2) the chairpersons and ranking minority members of—

(A) the Committee on Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate; and

(B) the Committee on Government Reform and the Committee on Small Business of the House of Representatives; and

(3) the Small Business and Agriculture Regulatory Enforcement Ombudsman designated under section 30(b) of the Small Business Act (15 U.S.C. 657 (b)).

(g) The task force shall terminate after completion of its work.

(h) In this section, the term “small business concern” has the meaning given under section 3 of the Small Business Act (15 U.S.C. 632).

Sec. 3521. Authorization of appropriations

There are authorized to be appropriated to the Office of Information and Regulatory Affairs to carry out the provisions of this subchapter, and for no other purpose, $8,000,000 for each of the fiscal years 1996, 1997, 1998, 1999, 2000, and 2001.

40 U.S.C. Subtitle III, Chapters 111, 113, 115, and 117

Also known as: Division D – Federal Acquisition Reform Act of 1996 and Division E – The Information Technology Management Reform Act of 1996 in the National Defense Authorization Act for Fiscal Year 1996; or the Clinger-Cohen Act of 1996.	
Public Law	104-106
Date	February 10, 1996, updated as of January 3, 2007
Reports	U.S. House. Conference Report. H. Report 104-450[5]

TITLE 40 - PUBLIC BUILDINGS, PROPERTY, AND WORKS

SUBTITLE III - INFORMATION TECHNOLOGY MANAGEMENT
CHAPTER 111 - GENERAL
CHAPTER 113 - RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY
CHAPTER 115 - INFORMATION TECHNOLOGY ACQUISITION PILOT PROGRAM
CHAPTER 117 - ADDITIONAL INFORMATION RESOURCES MANAGEMENT MATTERS

TITLE 40 - SUBTITLE III - CHAPTER 111 - GENERAL

§ 11101. Definitions
§ 11102. Sense of Congress
§ 11103. Applicability to national security systems

TITLE 40 - SUBTITLE III - CHAPTER 113 - RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

SUBCHAPTER I - DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET
SUBCHAPTER II - EXECUTIVE AGENCIES
SUBCHAPTER III - OTHER RESPONSIBILITIES

TITLE 40 - SUBTITLE III - CHAPTER 113

[5] An earlier version of the legislation (H.R. 1530/S. 1026) was vetoed by the President on December 22, 1995. U.S. House, Committee on National Security, H. Report No. 104-131; U.S. Senate, Committee on Armed Services, S. Report No. 104-112; U.S. House, Conference Report, H. Report No. 104-406

40 U.S.C. Subtitle III, Chapters 111, 113, 115, and 117

SUBCHAPTER I - DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET

§ 11301. Responsibility of Director
§ 11302. Capital planning and investment control
§ 11303. Performance-based and results-based management

TITLE 40 - SUBTITLE III - CHAPTER 113

SUBCHAPTER II - EXECUTIVE AGENCIES

§ 11311. Responsibilities
§ 11312. Capital planning and investment control
§ 11313. Performance and results-based management
§ 11314. Authority to acquire and manage information technology
§ 11315. Agency Chief Information Officer
§ 11316. Accountability
§ 11317. Significant deviations
§ 11318. Interagency support

TITLE 40 - SUBTITLE III - CHAPTER 113

SUBCHAPTER III- OTHER RESPONSIBILITIES

§ 11331. Responsibilities for Federal information systems standards
[§ 11332. Repealed.]

TITLE 40 - SUBTITLE III - CHAPTER 115 - INFORMATION TECHNOLOGY ACQUISITION PILOT PROGRAM

SUBCHAPTER I - CONDUCT OF PILOT PROGRAM
SUBCHAPTER II - SPECIFIC PILOT PROGRAM

TITLE 40 - SUBTITLE III - CHAPTER 115

SUBCHAPTER I - CONDUCT OF PILOT PROGRAM

§ 11501. Authority to conduct pilot program

§ 11502. Evaluation criteria and plans

§ 11503. Report

§ 11504. Recommended legislation

§ 11505. Rule of construction

TITLE 40 - SUBTITLE III - CHAPTER 115

SUBCHAPTER II - SPECIFIC PILOT PROGRAM

[§ 11521. Repealed.]

[§ 11522. Repealed.]

TITLE 40 - SUBTITLE III - CHAPTER 117 - ADDITIONAL INFORMATION RESOURCES MANAGEMENT MATTERS

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11101. Definitions

In this subtitle, the following definitions apply:

(1) Commercial item.- The term "commercial item" has the meaning given that term in section 4 of the Office of Federal Procurement Policy Act (41 U.S.C. 403).

(2) Executive agency.- The term "executive agency" has the meaning given that term in section 4 of the Act (41 U.S.C. 403).

(3) Information resources.- The term "information resources" has the meaning given that term in section 3502 of title 44.

(4) Information resources management.- The term "information resources management" has the meaning given that term in section 3502 of title 44.

(5) Information system.- The term "information system" has the meaning given that term in section 3502 of title 44.

(6) Information technology.- The term "information technology"-

(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use –

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peri-

pheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11102. Sense of Congress

It is the sense of Congress that, during the five-year period beginning with 1996, executive agencies should achieve each year through improvements in information resources management by the agency-

(1) at least a five percent decrease in the cost (in constant fiscal year 1996 dollars) incurred by the agency in operating and maintaining information technology; and

(2) a five percent increase in the efficiency of the agency operations.

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11103. Applicability to national security systems

(a) Definition.-

(1) National security system. - In this section, the term "national security system" means a telecommunications or information system operated by the Federal Government, the function, operation, or use of which –

(A) involves intelligence activities;

(B) involves cryptologic activities related to national security;

(C) involves command and control of military forces;

(D) involves equipment that is an integral part of a weapon or weapons system; or

(E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

(2) Limitation.- Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(b) In General.- Except as provided in subsection (c), chapter 113 of this title does not apply to national security systems.

(c) Exceptions.-

(1) In general.- Sections 11313, 11315, and 11316 of this title apply to national security systems.

(2) Capital planning and investment control.- The heads of executive agencies shall apply sections 11302 and 11312 of this title to national security systems to the extent practicable.

(3) Applicability of performance-based and results-based management to national security systems.

(A) In general.- Subject to subparagraph (B), the heads of executive agencies shall apply section 11303 of this title to national security systems to the extent practicable.

(B) Exception.-National security systems are subject to section 11303 (b)(5) of this title, except for subparagraph (B)(iv).

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER I -

§ 11301. Responsibility of Director

In fulfilling the responsibility to administer the functions assigned under chapter 35 of title 44, the Director of the Office of Management and Budget shall comply with this chapter with respect to the specific matters covered by this chapter.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER I -

§ 11302. Capital planning and investment control

(a) Federal Information Technology.- The Director of the Office of Management and Budget shall perform the responsibilities set forth in this section in fulfilling the responsibilities under section 3504 (h) of title 44.

(b) Use of Information Technology in Federal Programs - The Director shall promote and improve the acquisition, use, and disposal of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

(c) Use of Budget Process -

(1) Analyzing, tracking, and evaluating capital investments.- As part of the budget process, the Director shall develop a process for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems. The process shall cover the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments.

(2) Report to Congress.- At the same time that the President submits the budget for a fiscal year to Congress under section 1105 (a) of title 31, the Director shall submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by executive agencies for information systems and how the benefits relate to the accomplishment of the goals of the executive agencies.

(d) Information Technology Standards.-The Director shall oversee the development and implementation of standards and guidelines pertaining to federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 11331 of this title and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(e) Designation of Executive Agents for Acquisitions - The Director shall designate the head of one or more executive agencies, as the Director considers appropriate, as executive agent for Government-wide acquisitions of information technology.

(f) Use of Best Practices in Acquisitions - The Director shall encourage the heads of the executive agencies to develop and use the best practices in the acquisition of information technology.

(g) Assessment of Other Models for Managing Information Technology - On a continuing basis, the Director shall assess the experiences of executive agencies, state and local governments, international organizations, and the private sector in managing information technology.

(h) Comparison of Agency Uses of Information Technology - The Director shall compare the performances of the executive agencies in using information technology and shall disseminate the comparisons to the heads of the executive agencies.

(i) Monitoring Training - The Director shall monitor the development and implementation of training in information resources management for executive agency personnel.

(j) Informing Congress - The Director shall keep Congress fully informed on the extent to which the executive agencies are improving the performance of agency programs and the accomplishment of the agency missions through the use of the best practices in information resources management.

(k) Coordination of Policy Development and Review - The Director shall coordinate with the Office of Federal Procurement Policy the development and review by the Administrator of the Office of Information and Regulatory Affairs of policy associated with federal acquisition of information technology.

§ 11303. Performance-based and results-based management

(a) In General.- The Director of the Office of Management and Budget shall encourage the use of performance-based and results-based management in fulfilling the responsibilities assigned under section 3504 (h) of title 44.

(b) Evaluation of Agency Programs and Investments.-

(1) Requirement.-The Director shall evaluate the information resources management practices of the executive agencies with respect to the performance and results of the investments made by the executive agencies in information technology.

(2) Direction for executive agency action. - The Director shall issue to the head of each executive agency clear and concise direction that the head of each agency shall -

(A) establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all of its major investments in information systems;

(B) determine, before making an investment in a new information system-

(i) whether the function to be supported by the system should be performed by the private sector and, if so, whether any component of the executive agency performing that function should be converted from a governmental organization to a private sector organization; or

(ii) whether the function should be performed by the executive agency and, if so, whether the function should be performed by a private sector source under contract or by executive agency personnel;

(C) analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes, as appropriate, before making significant investments in information technology to be used in support of those missions; and

(D) ensure that the information security policies, procedures, and practices are adequate.

(3) Guidance for multiagency investments.- The direction issued under paragraph (2) shall include guidance for undertaking efficiently and effectively interagency and Federal Government-wide investments in information technology to improve the accomplishment of missions that are common to the executive agencies.

(4) Periodic reviews - The Director shall implement through the budget process periodic reviews of selected information resources management activities of the executive agencies to ascertain the efficiency and effectiveness of information technology in improving the performance of the executive agency and the accomplishment of the missions of the executive agency.

(5) Enforcement of accountability.-

(A) In general.- The Director may take any action that the Director considers appropriate, including an action involving the budgetary process or appropriations management process, to enforce accountability of the head of an executive agency for information resources management and for the investments made by the executive agency in information technology.

(B) Specific actions - Actions taken by the Director may include -

(i) recommending a reduction or an increase in the amount for information resources that the head of the executive agency proposes for the budget submitted to Congress under section 1105 (a) of title 31;

(ii) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources;

(iii) using other administrative controls over appropriations to restrict the availability of amounts for information resources; and

(iv) designating for the executive agency an executive agent to contract with private sector sources for the performance of information resources management or the acquisition of information technology.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11311. Responsibilities

In fulfilling the responsibilities assigned under chapter 35 of title 44, the head of each executive agency shall comply with this subchapter with respect to the specific matters covered by this subchapter.

§ 11312. Capital planning and investment control

(a) Design of Process. - In fulfilling the responsibilities assigned under section 3506 (h) of title 44, the head of each executive agency shall design and implement in the executive agency a process for maximizing the value, and assessing and managing the risks, of the information technology acquisitions of the executive agency.

(b) Content of Process.- The process of an executive agency shall -

(1) provide for the selection of information technology investments to be made by the executive agency, the management of those investments, and the evaluation of the results of those investments;

(2) be integrated with the processes for making budget, financial, and program management decisions in the executive agency;

(3) include minimum criteria to be applied in considering whether to undertake a particular investment in information systems, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information systems investment projects;

(4) identify information systems investments that would result in shared benefits or costs for other federal agencies or state or local governments;

(5) identify quantifiable measurements for determining the net benefits and risks of a proposed investment; and

(6) provide the means for senior management personnel of the executive agency to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11313. Performance and results-based management

In fulfilling the responsibilities under section 3506 (h) of title 44, the head of an executive agency shall -

(1) establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology;

(2) prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals;

(3) ensure that performance measurements -

(A) are prescribed for information technology used by, or to be acquired for, the executive agency; and

(B) measure how well the information technology supports programs of the executive agency;

(4) where comparable processes and organizations in the public or private sectors exist, quantitatively benchmark agency process performance against those processes in terms of cost, speed, productivity, and quality of outputs and outcomes;

(5) analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology to be used in support of the performance of those missions; and

(6) ensure that the information security policies, procedures, and practices of the executive agency are adequate.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11314. Authority to acquire and manage information technology

(a) In General.- The authority of the head of an executive agency to acquire information technology includes-

(1) acquiring information technology as authorized by law;

(2) making a contract that provides for multiagency acquisitions of information technology in accordance with guidance issued by the Director of the Office of Management and Budget; and

(3) if the Director finds that it would be advantageous for the Federal Government to do so, making a multiagency contract for procurement of commercial items of information technology that requires each executive agency covered by the contract, when procuring those items, to procure the items under that contract or to justify an alternative procurement of the items.

(b) FTS 2000 Program.— The Administrator of General Services shall continue to manage the FTS 2000 program, and to coordinate the follow-on to that program, for and with the advice of the heads of executive agencies.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11315. Agency Chief Information Officer

(a) Definition.- In this section, the term "information technology architecture", with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals.

(b) General Responsibilities - The Chief Information Officer of an executive agency is responsible for -

(1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this subtitle, consistent with chapter 35 of title 44 and the priorities established by the head of the executive agency;

(2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and

(3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

(c) Duties and Qualifications.- The Chief Information Officer of an agency listed in section 901 (b) of title 31—

(1) has information resources management duties as that official's primary duty;

(2) monitors the performance of information technology programs of the agency, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the head of the agency regarding whether to continue, modify, or terminate a program or project; and

(3) annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31) under section 306 of title 5 and sections 1105 (a)(28), 1115–1117, and 9703 (as added by section 5(a) of the Government Performance and Results Act of 1993 (Public Law 103–62, 107 Stat. 289)) of title 31-

(A) assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management;

(B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements;

(C) develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements; and

(D) reports to the head of the agency on the progress made in improving information resources management capability.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11316. Accountability

The head of each executive agency, in consultation with the Chief Information Officer and the Chief Financial Officer of that executive agency (or, in the case of an executive agency without a chief financial officer, any comparable official), shall establish policies and procedures to ensure that

(1) the accounting, financial, asset management, and other information systems of the executive agency are designed, developed, maintained, and used effect-

tively to provide financial or program performance data for financial statements of the executive agency;

(2) financial and related program performance data are provided on a reliable, consistent, and timely basis to executive agency financial management systems; and

(3) financial statements support -

(A) assessments and revisions of mission-related processes and administrative processes of the executive agency; and

(B) measurement of the performance of investments made by the agency in information systems.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11317. Significant deviations

The head of each executive agency shall identify in the strategic information resources management plan required under section 3506 (b)(2) of title 44 any major information technology acquisition program, or any phase or increment of that program, that has significantly deviated from the cost, performance, or schedule goals established for the program.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11318. Interagency support

The head of an executive agency may use amounts available to the agency for oversight, acquisition, and procurement of information technology to support jointly with other executive agencies the activities of interagency groups that are established to advise the Director of the Office of Management and Budget in carrying out the Director's responsibilities under this chapter. The use of those amounts for that purpose is subject to requirements and limitations on uses and amounts that the Director may prescribe. The Director shall prescribe the requirements and limitations during the Director's review of the executive agency's proposed budget submitted to the Director by the head of the executive agency for purposes of section 1105 of title 31.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER III -

§ 11331. Responsibilities for Federal information systems standards

(a) Definition. In this section, the term "information security" has the meaning given that term in section 3532 (b)(1) of title 44.

(b) Requirement to Prescribe Standards. -

(1) In general.-

(A) Requirement.- Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–

(a) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) Required standards. - Standards promulgated under subparagraph (A) shall include -

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (b)); and

(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

(C) Required standards binding.- Information security standards described under subparagraph (B) shall be compulsory and binding.

(2) Standards and guidelines for national security systems.- Standards and guidelines for national security systems, as defined under section 3532 (3) of title 44, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(c) Application of More Stringent Standards**.-** The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards -

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44.

(d) Requirements Regarding Decisions by Director -

(1) Deadline.- The decision regarding the promulgation of any standard by the Director under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(2) Notice and comment.- A decision by the Director to significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER III -

§ 11332. Repealed. Pub. L. 107–296, title X, § 1005(a)(1), Nov. 25, 2002, 116 Stat. 2272; Pub. L. 107–347, title III, § 305(a), Dec. 17, 2002, 116 Stat. 2960] Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1244, related to Federal computer system security training and plan.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11501. Authority to conduct pilot program

(a) In General -

(1) Purpose - In consultation with the Administrator for the Office of Information and Regulatory Affairs, the Administrator for Federal Procurement Policy may conduct a pilot program pursuant to the requirements of section 11521 of this title to test alternative approaches for the acquisition of information technology by executive agencies.

(2) Multiagency, multi-activity conduct of each program.— Except as otherwise provided in this chapter, the pilot program conducted under this chapter shall be carried out in not more than two procuring activities in each of the executive agencies that are designated by the Administrator for Federal Procurement Policy in accordance with this chapter to carry out the pilot program. With the approval of the Administrator for Federal Procurement Policy, the head of each designated executive agency shall select the procuring activities of the executive agency that are to participate in the test and shall designate a procurement testing official who shall be responsible for the conduct and evaluation of the pilot program within the executive agency.

(b) Limitation on Amount.— The total amount obligated for contracts entered into under the pilot program conducted under this chapter may not exceed $375,000,000. The Administrator for Federal Procurement Policy shall monitor those contracts and ensure that contracts are not entered into in violation of this subsection.

(c) Period of Programs -

(1) In general.- Subject to paragraph (2), the pilot program may be carried out under this chapter for the period, not in excess of five years, the Administrator for Federal Procurement Policy determines is sufficient to establish reliable results.

(2) Continuing validity of contracts.- A contract entered into under the pilot program before the expiration of that program remains in effect according to the terms of the contract after the expiration of the program.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11502. Evaluation criteria and plans

(a) Measurable Test Criteria.- To the maximum extent practicable, the head of each executive agency conducting the pilot program under section 11501 of this title shall establish measurable criteria for evaluating the effects of the procedures or techniques to be tested under the program.

(b) Test Plan.- Before the pilot program may be conducted under section 11501 of this title, the Administrator for Federal Procurement Policy shall submit to Congress a detailed test plan for the program, including a detailed description of the procedures to be used and a list of regulations that are to be waived.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11503. Report

(a) Requirement.— Not later than 180 days after the completion of the pilot program under this chapter, the Administrator for Federal Procurement Policy shall-

(1) submit to the Director of the Office of Management and Budget a report on the results and findings under the program; and

(2) provide a copy of the report to Congress.

(b) Content.- The report shall include

(1) a detailed description of the results of the program, as measured by the criteria established for the program; and

(2) a discussion of legislation that the Administrator recommends, or changes in regulations that the Administrator considers necessary, to improve overall information resources management in the Federal Government.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11504. Recommended legislation

If the Director of the Office of Management and Budget determines that the results and findings under the pilot program under this chapter indicate that legislation is necessary or desirable to improve the process for acquisition of information technology, the Director shall transmit the Director's recommendations for that legislation to Congress.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11505. Rule of construction

This chapter does not authorize the appropriation or obligation of amounts for the pilot program authorized under this chapter.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER II -

§11521. Repealed. Pub. L. 107–347, title II, §210(h)(1), Dec. 17, 2002, 116 Stat. 2938]

Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1247, related to the share-in-savings pilot program.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER II -

§ 11522. **Repealed. Pub.** L. 107–314, div. A, title VIII, § 825(b)(1), Dec. 2, 2002, 116 Stat. 2615]

Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1247, related to a pilot program to test the feasibility of using solutions-based contracting for the acquisition of information technology. Subsequent to repeal, Pub. L. 107–347, title II, § 210(h)(3)(A), Dec. 17, 2002, 116 Stat. 2938, directed that this section be renumbered section 11521 of this title.

TITLE 40 - SUBTITLE III - CHAPTER 117 -

§ 11701. Identification of excess and surplus computer equipment

In accordance with chapter 5 of this title, the head of an executive agency shall maintain an inventory of all computer equipment under the control of that official that is excess or surplus property.

TITLE 40 - SUBTITLE III - CHAPTER 117

§ 11702. Index of certain information in information systems included in directory established under section 4101 of title 44

If in designing an information technology system pursuant to this subtitle, the head of an executive agency determines that a purpose of the system is to disseminate information to the public, then the head of that executive agency shall reasonably ensure that an index of information disseminated by the system is included in the directory created pursuant to section 4101 of title 44. This section does not authorize the dissemination of information to the public unless otherwise authorized.

TITLE 40 - SUBTITLE III - CHAPTER 117

§ 11703. Procurement procedures

To the maximum extent practicable, the Federal Acquisition Regulatory Council shall ensure that the process for acquisition of information technology is a simplified, clear, and understandable process that specifically addresses the management of risk, incremental acquisitions and the need to incorporate commercial information technology in a timely manner.

House of Representatives Report 104-450 Conference Report

DIVISION E--INFORMATION TECHNOLOGY MANAGEMENT REFORM

LEGISLATIVE PROVISIONS

LEGISLATIVE PROVISIONS ADOPTED

Overview

The Senate amendment contained provisions with government-wide acquisition and management issues related to information technology. The House bill also contained provisions relating to bid protest jurisdictions. The conferees considered all of these provisions before agreeing to include Division E in the conference agreement.

The conferees agree that:

(1) federal information systems are critical to the lives of every American;

(2) the efficiency and effectiveness of the federal government is dependent upon the effective use of information;

(3) the federal government annually spends billions of dollars operating obsolete information systems;

(4) the use of obsolete information systems severely limits the quality of the services that the federal government provides, the efficiency of federal government operations, and the capabilities of the federal government to account for how taxpayer dollars are spent;

(5) the failure to modernize federal government information systems and the operations they support, despite efforts to do so, has resulted in the waste of billions of dollars that cannot be recovered;

(6) despite improvements achieved through implementation of the Chief Financial Officers Act of 1990, most federal agencies cannot track the expenditures of Federal dollars and, thus, expose the taxpayers to billions of dollars in waste, fraud, abuse, and mismanagement;

(7) poor planning and program management and an overburdened acquisition process have resulted in the American taxpayers not getting their money's worth from the expenditure of $200,000,000,000 on information systems during the decade preceding the enactment of this Act;

(8) the federal government's investment control processes focus too late in the system lifecycle, lack sound capital planning, and pay inadequate attention to business process improvement, performance measurement, project milestones, or benchmarks against comparable organizations;

(9) many federal agencies lack adequate personnel with the basic skills necessary to effectively and efficiently use information technology and other information resources in support of agency programs and missions;

(10) federal regulations governing information technology acquisitions are outdated, focus on paperwork and process rather than results, and prevent the federal government from taking timely advantage of the rapid advances taking place in the competitive and fast changing global information technology industry;

(11) buying, leasing, or developing information systems should be a top priority for federal agency management because of the high potential for the systems to substantially improve Federal Government operations, including the delivery of services to the public; and,

(12) structural changes in the federal government, including elimination of the Brooks Act (section 111 of the Federal Property and Administrative Services Act of 1949, as amended), are necessary in order to improve federal information management and to facilitate federal government acquisition of the state-of-the-art information technology that is critical for improving the efficiency and effectiveness of federal government operations.

The conferees agree that action is necessary on the part of Congress in order to:

(1) create incentives for the federal government to strategically use information technology in order to achieve efficient and effective operations of the federal government, and to provide cost effective and efficient delivery of federal government services to the taxpayers;

(2) provide for the cost effective and timely acquisition, management, and use of effective information technology solutions;

(3) transform the process-oriented procurement system of the federal government, as it relates to the acquisition of information technology, into a results-oriented procurement system;

(4) increase the responsibility and authority of officials of the Office of Management and Budget and other federal government agencies, and the account-

ability of such officials to Congress and the public, in the use of information technology and other information resources in support of agency missions;

(5) ensure that federal government agencies are responsible and accountable for achieving service delivery levels and project management performance comparable to the best in the private sector;

(6) promote the development and operation of multiple-agency and governmentwide, inter-operable, shared information resources to support the performance of federal government missions;

(7) reduce fraud, waste, abuse, and errors resulting from a lack of, or poor implementation of, federal government information systems;

(8) increase the capability of the federal government to restructure and improve processes before applying information technology;

(9) increase the emphasis placed by federal agency managers on completing effective capital planning and process improvement before applying information technology to the executing of plans and the performance of agency missions;

(10) coordinate, integrate, and, to the extent practicable, establish uniform federal information resources management policies and practices in order to improve the productivity, efficiency, and effectiveness of federal government programs and the delivery of services to the public;

(11) strengthen the partnership between the federal government and state, local, and tribal governments for achieving federal government missions, goals, and objectives;

(12) provide for the development of a well-trained core of professional federal government information resources managers; and,

(13) improve the ability of agencies to share expertise and best practices and coordinate the development of common application systems and infrastructure.

The following is a section-by-section description of the provisions adopted by the conferees.

Section 5001 sets forth a short title `The Information Technology Management Reform Act of 1996' and Section 5002 sets forth definitions.

TITLE LI--RESPONSIBILITY FOR ACQUISITION OF INFORMATION TECHNOLOGY

SUBTITLE A--GENERAL AUTHORITY

Repeal of central authority of the Administrator of General Services (sec. 5101)

The conference agreement includes a provision that would repeal section 111 of the Federal Property and Administrative Services Act of 1949, as amended.

SUBTITLE B--DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET

Responsibility of Director (sec. 5111)

The conference agreement includes a provision that would require the Director of the Office of Management and Budget to comply with this title. The conferees anticipate that these provisions will be reviewed upon reauthorization of the Paperwork Reduction Act prior to September 30, 2001.

The conferees agree that in undertaking activities and issuing guidance in accordance with this subtitle, the Director shall promote the integration of information technology management with the broader information resource management processes in the agencies. The conferees encourage the establishment of interagency groups to support the Director by examining areas of information technology, to include: telecommunications, software engineering, common administrative and programmatic applications, computer security and information policy, all of which would benefit from a government-wide or multiagency perspective; the promotion of cooperation among agencies in information technology matters; the review of major or high risk information technology acquisitions; and the promotion of the efficient use of information technology that supports agency missions. The interagency groups should: identify common goals and requirements; develop a coordinated approach to meeting certain agency requirements, such as budget estimates and procurement programs; identify opportunities to share information that would improve the agency performance and reduce costs of agency programs; make recommendations regarding protocols and other standards for information technology, including security standards; and make recommendations concerning interoperability among agency information systems. The conferees also encourage the establishment of temporary special advisory groups, composed of experts from industry, academia, and the Federal Government, to review government-wide information technology programs, major or high risk information technology acquisitions, and information technology policy.

Capital planning and investment control (sec. 5112)

The conference agreement includes a provision that would describe the Director's responsibilities under 44 USC 3504(h) that relate to promoting and sustaining responsibility and accountability for improvement of the acquisition, use, and disposal of information technology by executive agencies.

The conferees agree that the Director, in developing a process related to major agency capital investments, should: ensure that the process identifies opportunities for interagency cooperation; ensure the success of high risk and high return investments; develop requirements for agency submission of investment information needed to execute the process; ensure that agency information resources management plans are integrated into the agency's program plans, financial management plans, and budgets for the acquisition and use of information technology designed to improve agency performance and the accomplishment of agency missions; and identify three categories of information systems investments--(1) high risk--those projects that, by virtue of their size, complexity, use of innovative technology, or other factors, have an especially high risk of failure; (2) high return--those projects that by virtue of their total potential benefits, in proportion to their costs, have particularly unique value to the public; and (3) crosscutting--those projects of individual agencies, with shared benefit to or impact on other federal agencies and state or local governments, that require enforcement of operational standards or elimination of redundancies. Finally, the conferees also agree that the Director, to encourage the use of best business and administrative practices, should identify and collect information regarding best practices, to include information on the development and implementation of best practices by the executive agencies. The Director should provide the executive agencies with information on best practices, and advice and assistance regarding the use of best practices.

Performance-based and results-based management (sec. 5113)

The conference agreement includes a provision that would require the Director to encourage performance and results-based management for agency information technology programs. The Director is required to review agency management practices based on the performance and results of its information technology programs and investments. The Director is required to issue clear and concise directions to ensure that agencies have effective and efficient capital planning processes that are used to select, control, and evaluate the results of major information systems investments and to ensure that agency information security is adequate. The conferees agree that the Director's direction to agencies regarding performance and

results based management of information technology resources shall contain the following: (1) that each executive agency and its major subcomponents institute effective and efficient capital planning processes for selecting, controlling, and evaluating the results of all of its major information systems investments; (2) that the agency maintain a current and adequate information resources management plan, and to the maximum extent practicable, specifically identify the method for acquisition of information technology expected to improve agency operations, and otherwise benefit the agency; (3) that the agency provide for adequate integration of the agency's information resources management plans, strategic plans prepared pursuant to 5 U.S.C. 306, performance plans prepared pursuant to 31 U.S.C. 1115, financial management plans prepared pursuant to 31 U.S.C. 902(a)(5), and the agency budgets for the acquisition and use of information technology and other information resources. In addition, the conferees agree that OMB shall provide the needed oversight, through the budget process and other means, to ensure that executive agencies assume responsibility, and effectively implement suitable performance and results-based management practices.

SUBTITLE C--EXECUTIVE AGENCIES

Responsibilities (sec. 5121)

The conference agreement includes a provision that would require the head of each executive agency to comply with this subtitle. The conferees anticipate that these provisions will be reviewed upon reauthorization of the Paperwork Reduction Act prior to September 30, 2001. The conferees encourage the establishment and support of independent technical review committees, composed of diverse agency personnel (including users) and outside experts selected by the agency head, to advise an agency head about information systems programs.

Capital planning and investment control (sec. 5122)

The conference agreement includes a provision that would require agencies to develop a process for furthering their responsibilities under 44 U.S.C. 3506(h). The head of the agency is required to design and develop a process for maximizing the value and assessing and managing the risk of the agency's information technology acquisitions.

Performance and results-based management (sec. 5123)

The conference agreement includes a provision that would require agencies to establish goals for and report on the progress of improving efficiency and

effectiveness of agency operations through use of information technology, as required by 44 U.S.C. 3506(h). The head of an executive agency must ensure that performance measures are established to support evaluating the results and benefits of information technology investments.

The conferees agree that, in fulfilling the responsibilities under this section, agency heads should ensure that: (1) before investing in information technology to support a function, the agency determines whether that function should be performed in the private sector or by an agency of the federal government; (2) the agency adequately provides for the integration of the agency's information resources management plans, strategic plans prepared pursuant to 5 U.S.C. 306, performance plans prepared pursuant to 31 U.S.C. 1115, financial management plans prepared pursuant to 31 U.S.C. 902(a)(5), and adequately prepares budgets for the acquisition and use of information technology; (3) the agency maintains a current and adequate information resources management plan, and to the maximum extent practicable, specifically identifies how acquired information technology would improve agency operations and otherwise benefit the agency; and (4) the agency invests in efficient and effective interagency and government-wide information technology to improve the accomplishment of common agency missions or functions.

Acquisitions of information technology (sec. 5124)

The conference agreement includes a provision that would authorize the head of an executive agency to acquire information technology and, upon approval of the Director of OMB, enter into multi-agency information technology investments. The conferees intend that the requirements and limitations of the Economy Act, and other provisions of law, apply to these multiagency acquisitions. This section also authorizes the General Services Administration (GSA) to continue the management of the FTS-2000 program and coordinate the follow-on effort to FTS-2000.

Agency chief information officer (sec. 5125)

The conference agreement includes a provision that would amend the Paperwork Reduction Act of 1995 by replacing the `senior information resources management official position' established within each executive agency with an agency Chief Information Officer (CIO). The agency CIO is responsible for providing information and advice regarding information technology and information resources management to the head of the agency, and for ensuring that

the management and acquisition of agency information technology is implemented consistent with the provisions of this law.

The conferees anticipate that agencies may establish CIOs for major subcomponents or bureaus, and expect agency CIOs will possess knowledge of, and practical experience in, information and information technology management practices of business or government entities. The conferees also intend that deputy chief information officers be appointed by agency heads that have additional experience in business process analysis, software and information systems development, design and management of information technology architectures, data and telecommunications management at government or business entities. The conferees intend that CIOs, in agencies other than those listed in 31 U.S.C. 901(b), perform essentially the same duties as CIOs in agencies listed in 31 U.S.C. 901(b). The conferees expect that an agency's CIO will meet periodically with other appropriate agency officials to advise and coordinate the information technology and other information resources management activities of the various agencies.

Accountability (sec. 5126)

The conference agreement includes a provision that would require the head of each agency, in consultation with agency Chief Information Officers and Chief Financial Officers, to ensure the integration of financial and information systems. The conferees intend that the information resources management plan, required under 44 U.S.C. 3506(b)(2), support the performance of agency missions through the application of information technology and other information resources, and include the following: (1) a statement of goals to improve the extent to which information resources contribute to program productivity, efficiency, and effectiveness; (2) the development of methods to measure progress toward achieving the goals; (3) the establishment of clear roles, responsibilities, and accountability to achieve the goals; (4) a description of an agency's major existing and planned information technology components (such as information systems and telecommunications networks); (5) the relationship among the information technology components, and the information architecture; and (6) a summary of the project's status and any changes in name, direction or scope, quantifiable results achieved, and current maintenance expenditures for each ongoing or completed major information systems investment from the previous year. The conferees also intend that agency heads will periodically evaluate and improve the accuracy, security, completeness, and reliability of information maintained by or for the agency.

Significant deviations (sec. 5127)

The conference agreement includes a provision that would require agencies to identify in their information resources management plans any major information technology acquisition program, or phase or increment of such program, that has significantly deviated from the established cost, performance, or schedule baseline.

Interagency support (sec. 5128)

The conference agreement includes a provision that would authorize the utilization of funds for interagency activities in support of the Information Technology Reform Act.

SUBTITLE D--OTHER RESPONSIBILITIES.

Responsibilities regarding efficiency, security, and privacy of federal computer systems (sec. 5131)

The conference agreement includes a provision that would set forth the authority for the Secretary of Commerce, in consultation with the National Institute of Standards and Technology, to promulgate standards to improve the operation, security, and privacy of Federal information technology systems.

Sense of Congress (sec. 5132)

The conference agreement includes a provision stating that agencies, over the next five years, should achieve a five percent per year decrease in costs incurred for operation and maintenance of information technology, and a five percent increase in operational efficiency through improvements in information resources management.

SUBTITLE E--NATIONAL SECURITY SYSTEMS

The conference agreement includes a provision that would exclude national security systems from provisions of this Act, unless otherwise provided in this Act.

TITLE LII--PROCESS FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

Procurement procedures (sec. 5201)

The conference agreement includes a provision that would direct the Federal Acquisition Regulatory Council to ensure, to the maximum extent practicable, that the information technology process is simplified, clear, and understandable. The process should specifically address the management of risk, incremental acquisitions, and the need to incorporate commercial information technology in a timely manner.

The conferees agree that, in performing oversight of information technology acquisitions, the Director of the Office of Management and Budget, agency heads, and agency inspectors general should emphasize program results and established performance measurements, rather than reviews of the acquisition process.

Incremental acquisition of information technology (sec. 5202)

The conference agreement includes a provision that would provide for procedures in the Federal Acquisition Regulations for the incremental acquisition of major information technology systems by the Department of Defense and the civilian executive agencies.

TITLE LIII--INFORMATION TECHNOLOGY ACQUISITION PILOT PROGRAMS

SUBTITLE A--CONDUCT OF PILOT PROGRAMS

The conference agreement includes provisions that would authorize the Administrator of Office of Federal Procurement Policy, in consultation with the Administrator of Office of Information and Regulatory Affairs, to: conduct pilot programs to test alternative acquisition approaches for information technology; conduct no more than two pilots, not to exceed $750 million for a period not to exceed five years; require agency heads to develop evaluation and test plans; prepare and submit test plans to Congress prior to implementation; report on results within 180 days after completion; and make recommendations for legislation.

SUBTITLE B--SPECIFIC PILOT PROGRAMS

The conference agreement includes provisions that would provide for two specific pilot programs, the share-in-savings pilot program and the solutions-based contracting pilot program.

TITLE LIV--ADDITIONAL INFORMATION RESOURCES MANAGEMENT MATTERS

On-line multiple award schedule contracting (sec. 5401)

The conference agreement includes a provision that would require the Administrator of General Services to provide for on-line access to multiple award schedules for information technology. The system would provide basic information on prices, features, and similar matters, allow for information updates, enable comparison of product information, enable on-line ordering and invoicing, permit on-line payment, and archive order data. The provision would also auth-

orize a pilot program to test streamlined procedures for the automated system. The conference agreement directs the Administrator of General Services to incorporate its information technology multiple award schedules into Federal Acquisition Computer Network (FACNET) by January 1, 1998, and would make the pilot program discretionary. The conferees agree that the procedures established by the Administrator for use of FACNET be consistent with the Federal Property and Administrative Services Act requirements regarding the multiple award schedule (41 U.S.C. 259(B)(3)). If the Administrator determines it is not practicable to provide such access through FACNET, the Administrator shall provide such access through another automated system that has the capability to perform the functions listed in subsection 259(b)(1) and meets the requirement of subsection 259(b)(2).

Disposal of excess computer equipment (sec. 5402)

The conference agreement includes a provision that would require agencies to inventory all agency computer equipment and to identify excess or surplus property. The conferees direct that the Administrator of General Services, in exercising current authority under title II of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 481 et seq.), donate federal surplus personal property to public organizations. The conferees direct the Administrator to prescribe regulations that establish a priority for the donation of surplus computer equipment in the following sequence: (1) elementary and secondary schools, and schools funded by the Bureau of Indian Affairs; (2) public libraries; (3) public colleges and universities; and (4) other entities eligible for donation of federal surplus personal property under title II of that Act.

Access of certain information in information systems to the directory established under section 4101 of title 44, United States Code (sec. 5403)

The conference agreement includes a provision that would ensure that, for agency information systems that disseminate information to the public, an index of information is included in the Government Printing Office (GPO) directory established under 44 U.S.C. 4101.

In 1993, Congress directed the GPO to create an online directory, of federal public information in electronic form (Public Law 103-40). Today, that system is accessible to the general public directly and through the Federal Depository Libraries. Yet, in the two years since enactment of the GPO access bill, technology has moved forward dramatically in its ability to support location and search of the

physically-distributed, locally-maintained databases. Congress recognized this shift in the Paperwork Reduction Act of 1995 (Public Law 104-13). That Act requires Federal agencies to ensure access to agency public information by ‘encouraging a diversity of public and private sources. It also directs the Office of Management and Budget to establish a distributed, electronic, agency-based Government Information Locator Service (GILS) to identify the major information dissemination products of each agency. As the Senate report noted (S. Rept. 104-112), GILS: `* * * will provide multiple avenues for public access to government information by pointing to specific agency information holdings. To make this possible, agencies' systems must be compatible. Thus, agency GILS information should be available to the public through the Government Printing Office Locator System (established pursuant to Public Law 103-40) in addition to any other required methods, agencies may choose to efficiently and effectively provide public and agency access to GILS.' Section 5403 further clarifies the intent of Congress to ensure the widest possible access to Federal public information through a diversity of compatible sources.

TITLE LV--PROCUREMENT PROTEST AUTHORITY OF THE COMPTROLLER GENERAL

The conference agreement includes a provision that would require the Comptroller General to issue a decision relating to a bid protest within 100 days.

TITLE LVI--CONFORMING AND CLERICAL AMENDMENTS

The conference agreement includes a series of clarifying and technical changes to acquisition statutes throughout the United States Code.

TITLE LVII--EFFECTIVE DATE, SAVINGS PROVISIONS, AND RULE OF CONSTRUCTION

Effective date (sec. 5701)

The conference agreement includes a provision that would provide for this division and the amendments made by this division to take effect 180 days after the date of the enactment of this Act.

Savings provisions (sec. 5702)

The conference agreement includes a provision that would allow selected information technology actions and acquisition proceedings, including claims or applications, that have been initiated by, or are pending before, Administrator of the General Services or the General Services Administration Board of Contract Appeals to be continued under original terms, until terminated, revoked, or

superseded in accordance with law, by the Director of OMB, by a court, or by operation of law. The Director of OMB is authorized to establish regulations for transferring such actions and proceedings.

Floyd Spence,
Bob Stump,
Duncan Hunter,
Herbert H. Bateman,
Curt Weldon,
G.V. Montgomery,
John M. Spratt, Jr.,
Managers on the Part of the House.
Strom Thurmond,
John Warner,
Bill Cohen,
Trent Lott,
Sam Nunn,
Managers on the Part of the Senate.

Office of Management and Budget Circular A-130

OMB Circular	No. A-130, "Management of Federal Information Resources," Transmittal Memorandum No. 4
Date	November 28, 2000

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

1. Purpose:

This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2. Rescissions:

This Circular rescinds OMB Memoranda M-96-20, "Implementation of the Information Technology Management Reform Act of 1996;" M-97-02, "Funding Information Systems Investments;" M-97-09, "Interagency Support for Information Technology;" M-97-15, "Local Telecommunications Services Policy;" M-97-16, "Information Technology Architectures."

3. Authorities:

OMB issues this Circular pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); the Computer Security Act of 1987 (Pub. L. 100-235); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); the Government Performance and Results Act of 1993 (GPRA); the Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), Executive Order No. 12046 of March 27, 1978; Executive Order No. 12472 of April 3, 1984; and Executive Order No. 13011 of July 17, 1996.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background:

The Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by

1. focusing information resource planning to support their strategic missions;

2. implementing a capital planning and investment control process that links to budget formulation and execution; and

3. rethinking and restructuring the way they do their work before investing in information systems.

The PRA establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the PRA requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the

development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.

c. The term "capital planning and investment control process " means a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

d. The term "Chief Information Officers Council" (CIO Council) means the Council established in Section 3 of Executive Order 13011.

e. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

f. The term "executive agency" has the meaning defined in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

g. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.

h. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

i. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

j. The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

k. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

l. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

m. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

n. The term "information resources" includes both government information and information technology.

o. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

p. The term "information resources management" means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

q. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

r. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

s. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition,

storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

t. The term "Information Technology Resources Board" (Resources Board) means the board established by Section 5 of Executive Order 13011.

u. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

v. The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget document preparation requirements set forth in OMB Circular A-11. The resultant budget document may be classified in accordance with the provisions of Executive Order 12958.

w. The term "records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or

characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

x. The term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposetion in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

y. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It provides the public with knowledge of the government, society, and economy -- past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the

Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations.

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Strategic planning improves the operation of government programs. The agency strategic plan will shape the redesign of work processes and guide the development and maintenance of an Enterprise Architecture and a capital planning and investment control process. This management approach promotes the appropriate application of Federal information resources

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

k. The open and efficient exchange of scientific and technical government information, subject to applicable national security controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

r. The Chief Information Officers Council and the Information Technology Resources Board will help in the development and operation of interagency and interoperable shared information resources to support the performance of government missions.

8. Policy:

a. Information Management Policy

1. How will agencies conduct Information Management Planning?

Agencies must plan in an integrated manner for managing information throughout its life cycle. Agencies will:

(a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;

(b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;

(c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;

(d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;

(f) Train personnel in skills appropriate to management of information;

(g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;

(h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;

(i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

(j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

(k) Incorporate records management and archival functions into the design, development, and implementation of information systems;

1. Provide for public access to records where required or appropriate.

2. What are the guidelines for Information Collection?

Agencies must collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

3. What are the guidelines for Electronic Information Collection?

Executive agencies under Sections 1703 and 1705 of the Government Paper-work Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide, by October 21, 2003, the (1) option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. Agencies will follow the provisions in OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act."

4. How must agencies implement Records Management?

Agencies will:

(a) Ensure that records management programs provide adequate and proper documentation of agency activities;

(b) Ensure the ability to access records regardless of form or medium;

(c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records; and

(d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

5. How must an agency provide information to the public?

Agencies have a responsibility to provide information to the public consistent with their missions. Agencies will discharge this responsibility by:

(a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts;

(c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and

(d) In determining whether and how to disseminate information to the public, agencies will:

(i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;

(ii) Disseminate information dissemination products on equitable and timely terms;

(iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

6. What is an Information Dissemination Management System?

Agencies will maintain and implement a management system for all information dissemination products which must, at a minimum:

(a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);

(b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;

(c) Establish and maintain inventories of all agency information dissemination products;

(d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;

(e) Identify in information dissemination products the source of the information, if from another agency;

(f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;

(g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);

(h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;

(i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination products that meet their respective needs;

(j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(k) Ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made.

7. How must agencies avoid improperly restrictive practices?

Agencies will:

(a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis;

(b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on the reuse, resale, or redissemination of Federal information dissemination products by the public; and,

(c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They must exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:

(i) Where statutory requirements are at variance with the policy;

(ii) Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;

(iii) Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing the agency's functions, including reaching members of the public whom the agency has a responsibility to inform; or

(iv) Where the Director of OMB determines an exception is warranted.

8. How will agencies carry out electronic information dissemination?

Agencies will use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

(a) The agency develops and maintains the information electronically;

(b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;

(c) The agency disseminates the product frequently;

(d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;

(e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

9. What safeguards must agencies follow?

Agencies will:

(a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate

conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

(d) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.

b. How Will Agencies Manage Information Systems and Information Technology?

(1) How will agencies use capital planning and investment control process?

Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide both strategic and operational IRM, IT planning, and the Enterprise Architecture by integrating the agency's IRM plans, strategic and performance plans prepared pursuant to the Government Performance and Results Act of 1993, financial management plans prepared pursuant to the Chief Financial Officer Act of 1990 (31 U.S.C. 902a5), acquisition under the Federal Acquisition Streamlining Act of 1994, and the agency's budget formulation and execution processes. The capital planning and investment control process includes all stages of capital programming, including planning, budgeting, procurement, management, and assessment.

As outlined below, the capital planning and investment control process has three components: selection, control, and evaluation. The process must be iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results (for further guidance on Capital Planning refer to OMB Circular A-11). The agency's capital planning and investment control process must build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture. The Capital Planning and Investment Control processes must be documented, and provided to OMB consistent with the budget process. The Enterprise Architecture must be documented and provided to OMB as significant changes are incorporated.

(a) What plans are associated with the capital planning and investment control process?

In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Infor-

mation Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

The IT Capital Plan is operational in nature, supports the goals and missions identified in the IRM Strategic Plan, is a living document, and must be updated twice yearly. This IT Capital Plan is the implementation plan for the budget year. The IT Capital Plan should also reflect the goals of the agency's Annual Performance Plan, the agency's Government Paperwork Elimination Act (GPEA) Plan, the agency's EA, and agency's business planning processes. The IT Capital Plan must be submitted annually to OMB with the agency budget submission. The IT Capital Plan must include the following components:

(i) A component, derived from the agency's capital planning and investment control process under OMB Circular A-11, Section 300 and the OMB Capital Programming Guide, that specifically includes all IT Capital Asset Plans for major information systems or projects. This component must also demonstrate how the agency manages its other IT investments, as required by the Clinger-Cohen Act.

(ii) A component that addresses two other sections of OMB Circular A-11: a section for Information on Financial Management, including the Report on Financial Management Activities and the Agency's Financial Management Plan, and a section entitled Information Technology, including the Agency IT Investment Portfolio.

(iii) A component, derived from the agency's capital planning and investment control process, that demonstrates the criteria it will use to select the investments into the portfolio, how it will control and manage the investments, and how it will evaluate the investments based on planned performance versus actual accomplishments.

(iv) A component that includes a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance.

(b) What must an agency do as part of the selection component of the capital planning process?

It must:

(i) Evaluate each investment in information resources to determine whether the investment will support core mission functions that must be performed by the Federal government;

(ii) Ensure that decisions to improve existing information systems or develop new information systems are initiated only when no alternative private sector or governmental source can efficiently meet the need;

(iii) Support work processes that it has simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology;

(iv) Reduce risk by avoiding or isolating custom designed components, using components that can be fully tested or prototyped prior to production, and ensuring involvement and support of users;

(v) Demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. The return may include improved mission performance in accordance with GPRA measures, reduced cost, increased quality, speed, or flexibility; as well as increased customer and employee satisfaction. The return should reflect such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes;

(vi) Prepare and update a benefit-cost analysis (BCA) for each information system throughout its life cycle. A BCA will provide a level of detail proportionate to the size of the investment, rely on systematic measures of mission performance, and be consistent with the methodology described in OMB Circular No. A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs";

(vii) Prepare and maintain a portfolio of major information systems that monitors investments and prevents redundancy of existing or shared IT capabilities. The portfolio will provide information demonstrating the impact of alternative IT investment strategies and funding levels, identify opportunities for sharing resources, and consider the agency's inventory of information resources;

(viii) Ensure consistency with Federal, agency, and bureau Enterprise architectures, demonstrating such consistency through compliance with agency business requirements and standards, as well as identification of milestones, as defined in the EA;

(ix) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector;

(x) Ensure that the selected system or process maximizes the usefulness of information, minimizes the burden on the public, and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information, as determined in accordance with the PRA and the Federal Records Act. This portion must specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(xi) Establish oversight mechanisms, consistent with Appendix III of this Circular, to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data;

(xii) Ensure that Federal information system requirements do not unnecessarily restrict the prerogatives of state, local and tribal governments;

(xiii) Ensure that the selected system or process facilitates accessibility under the Rehabilitation Act of 1973, as amended.

(c) What must an agency do as part of the control component of the capital planning process? It must:

(i) Institute performance measures and management processes that monitor actual performance compared to expected results. Agencies must use a performance based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality;

(ii) Establish oversight mechanisms that require periodic review of information systems to determine how mission requirements might have changed, and whether the information system continues to fulfill ongoing and anticipated mission requirements. These mechanisms must also require information regarding the future levels of performance, interoperability, and maintenance necessary to ensure the information system meets mission requirements cost effectively;

(iii) Ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle. Information systems must also continue to deliver intended benefits to the agency and customers, meet user requirements, and identify and offer security protections;

(iv) Prepare and update a strategy that identifies and mitigates risks associated with each information system;

(iv) Ensure that financial management systems conform to the requirements of OMB Circular No. A-127, "Financial Management Systems;"

(v) Provide for the appropriate management and disposition of records in accordance with the Federal Records Act.

(vi) Ensure that agency EA procedures are being followed. This includes ensuring that EA milestones are reached and documentation is updated as needed.

(d) What must an agency do as part of the evaluation component of the capital planning process?

It must:

(i) Conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use;

(ii) Evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements.

(iii) Document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge.

(iv) Re-assess an investment's business case, technical compliance, and compliance against the EA.

(v) Update the EA and IT capital planning processes as needed.

(2) The Enterprise Architecture

Agencies must document and submit their initial EA to OMB. Agencies must submit updates when significant changes to the Enterprise Architecture occur.

(a) What is the Enterprise Architecture?

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information tech-

nology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the road-map for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with GPEA, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. Agencies must implement the EA consistent with following principles:

(i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;

(ii) Meet information technology needs through cost effective intra-agency and interagency sharing, before acquiring new information technology resources; and

(iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

(b) How do agencies create and maintain the EA?

As part of the EA effort, agencies must use or create an Enterprise Architecture Framework. The Framework must document linkages between mission needs, information content, and information technology capabilities. The Framework must also guide both strategic and operational IRM planning.

Once a framework is established, an agency must create the EA. In the creation of an EA, agencies must identify and document:

(i) Business Processes - Agencies must identify the work performed to support its mission, vision and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive changes in the EA.

(ii) Information Flow and Relationships - Agencies must analyze the information utilized by the agency in its business processes, identifying the information

used and the movement of the information. These information flows indicate where the information is needed and how the information is shared to support mission functions.

(iii) Applications - Agencies must identify, define, and organize the activities that capture, manipulate, and manage the business information to support business processes. The EA also describes the logical dependencies and relationships among business activities.

(iv) Data Descriptions and Relationships - Agencies must identify how data is created, maintained, accessed, and used. At a high level, agencies must define the data and describe the relationships among data elements used in the agency's information systems.

(v) Technology Infrastructure - Agencies must describe and identify the functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.

(c) What are the Technical Reference Model and Standards Profile?

The EA must also include a Technical Reference Model (TRM) and Standards Profile.

(i) The TRM identifies and describes the information services (such as database, communications, intranet, etc.) used throughout the agency.

(ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.

(iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

(3) How Will Agencies Ensure Security in Information Systems?

Agencies must incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems.

(a) To support more effective agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:

(i) Prioritize key systems (including those that are most critical to agency operations);

(ii) Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

(b) Agencies must make security's role explicit in information technology investments and capital programming. Investments in the development of new or the continued operation of existing information systems, both general support systems and major applications must:

(i) Demonstrate that the security controls for components, applications, and systems are consistent with, and an integral part of, the EA of the agency;

(ii) Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;

(iii) Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;

(iv) Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;

(v) Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;

(vi) Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

(vii) Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access;

(viii) Ensure that the handling of personal information is consistent with relevant government-wide and agency policies;

(ix) Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications;

(c) OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

(4) How Will Agencies Acquire Information Technology?

Agencies must:

(a) Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information technology;

(b) Structure major information systems into useful segments with a narrow scope and brief duration. This should reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;

(c) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes; and

(d) Ensure accessibility of acquired information technology pursuant to the Rehabilitation Act of 1973, as amended (Pub. Law 105-220, 29 U.S.C.794d).

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency must:

1. Have primary responsibility for managing agency information resources;

2. Ensure that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB;

3. Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger-Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and will advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things:

(a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans;

(b) Advise the agency head on information resource implications of strategic planning decisions;

(c) Advise the agency head on the design, development, and implementation of information resources.

(i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project;

(ii) Advise the agency head on budgetary implications of information resource decisions; and

(d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources;

4. Direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with this Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1st of each year.

5. Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

6. Develop agency policies and procedures that provide for timely acquisition of required information technology;

7. Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511) and the Freedom of Information Act (5 U.S.C. 552(g)): an inventory of the agency's major information systems, holdings, and dissemination products; an agency information locator service; a description of the agency's major information and record locator systems; an inventory of the agency's other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency's information resources); and a handbook for persons to obtain public information from the agency pursuant to these Acts.

8. Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

9. Identify to the Director of OMB any statutory, regulatory, and other impedements to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

10. Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

11. Ensure that the agency:

(a) cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs;

(b) promotes a coordinated, interoperable, secure, and shared government wide infrastructure that is provided and supported by a diversity of private sector suppliers; and

(c) develops a well-trained corps of information resource professionals.

12. Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization;

13. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,

14. Ensure, to the extent reasonable, that in the design of information systems with the purpose of disseminating information to the public, an index of information disseminated by the system will be included in the directory created by the Superintendent of Documents pursuant to 41 U.S.C. 4101. (Nothing in this paragraph authorizes the dissemination of information to the public unless otherwise authorized.)

15. Permit, to the extent practicable, the use of one agency's contract by another agency or the award of multi-agency contracts, provided the action is within the scope of the contract and consistent with OMB guidance; and

16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

b. Department of State. The Secretary of State must:

1. Advise the Director of OMB on the development of United States positions and policies on international information policy and technology issues affecting

Federal government activities and the development of international information technology standards; and

2. Be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including federal information technology. The Secretary must also ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. These responsibilities may also require the Secretary to consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

c. Department of Commerce. The Secretary of Commerce must:

1. Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology, while taking into consideration the recommendations of the agencies and the CIO Council;

2. Advise the Director of OMB on the development of policies relating to the procurement and management of Federal telecommunications resources;

3. Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

4. Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;

5. Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

6. Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

7. Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director of OMB on such activities.

d. Department of Defense. The Secretary of Defense will develop, in consultation with the Administrator of General Services, uniform Federal telecommunications

standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services must:

1. Continue to manage the FTS2001 program and coordinate the follow-up to that program, on behalf of and with the advice of agencies;

2. Develop, maintain, and disseminate for the use of the Federal community (as requested by OMB or the agencies) recommended methods and strategies for the development and acquisition of information technology;

3. Conduct and manage outreach programs in cooperation with agency managers;

4. Be a liaison on information resources management (including Federal information technology) with State and local governments. GSA must also be a liaison with non-governmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5. Support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations on information resource management matters;

6. Provide support and assistance to the CIO Council and the Information Technology Resources Board.

7. Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act, as amended;

f. Office of Personnel Management. The Director, Office of Personnel Management, will:

1. Develop and conduct training programs for Federal personnel on information resources management, including end-user computing;

2. Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

3. Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States will:

1. Administer the Federal records management program in accordance with the National Archives and Records Act;

2. Assist the Director of OMB in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget will:

1. Provide overall leadership and coordination of Federal information resources management within the executive branch;

2. Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

3. Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

4. Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

5. Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3; 6. Develop and maintain a Governmentwide strategic plan for information resources management.

7. Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

8. Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;

9. Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes;

10. Review proposed U.S. Government Position and Policy statements on international issues affecting Federal Government information activities, and advise the Secretary of State as to their consistency with Federal information resources management policy.

11. Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy,

and policies regarding management of financial management systems with the Office of Federal Financial Management.

12. Evaluate agency information resources management practices and programs and, as part of the budget process, oversee agency capital planning and investment control processes to analyze, track, and evaluate the risks and results of major capital investments in information systems;

13. Notify an agency if OMB believes that a major information system project requires outside assistance;

14. Provide guidance on the implementation of the Clinger-Cohen Act and on the management of information resources to the executive agencies, to the CIO Council, and to the Information Technology Resources Board; and

15. Designate one or more heads of executive agencies as executive agent for government-wide acquisitions of information technology.

10. Oversight:

a. The Director of OMB will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

b. The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.

11. Effectiveness: This Circular is effective upon issuance. Nothing in this Circular will be construed to confer a private right of action on any person.

12. Inquiries: All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.

13. Sunset Review Date: OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.

OMB Circular A-11

OMB Circular A-11, Section 53	No. A-11, Preparation, Submission and Execution of the Budget, Section 53, Information Technology and E-Government
Date	November 11, 2008

Table of Contents

Summary of Changes

Updates definition of major IT acquisition/investment (section 53.3). Adds new columns to identify the mode of delivery, investment certification and accreditation status, and project manager qualification status (exhibit 53). Removes total investment column (exhibit 53).

53.1 Why must I report on information technology (IT) investments?

The information required allows the agency and OMB to review and evaluate each agency's IT spending and to compare IT spending across the Federal Government. Specifically the information helps the agency and OMB to:

• Ensure initiatives create a citizen-centered electronic presence and advance an E-Government (EGov) strategy including specific outcomes to be achieved;

• Understand the amount being spent on development and modernization of IT versus the amount being spent on operating and maintaining the status quo for IT;

• Identify costs for providing IT security as part of agency investment life cycle as well as IT security costs for supporting crosscutting or infrastructure related investments under the Federal Information Security Management Act (FISMA);

• Provide a full and accurate accounting of IT investments for the agency as required by the Clinger-Cohen Act of 1996;

• Ensure spending on IT supports agency compliance with the requirements of Section 508 of the Rehabilitation Act Amendments of 1998 (Electronic and Information Technology Accessibility) and Section 504 of the Rehabilitation Act of 1973 (Reasonable Accommodation);

• Ensure compliance with E-Government Act of 2002 and Paperwork Reduction Act of 1995;

• Ensure privacy is considered and protected in electronic activities;

• Identify investments supporting Homeland Security goals and objectives; and

• Review requests for agency financial management systems. Agencies must provide this information using the Agency IT Investment Portfolio (exhibit 53) reporting format. This information should be consistent with information required in section 51.3. In addition, as an output of your agency's internal capital planning and investment control process, your Budget justification for IT must provide results oriented information in the context of the agency's missions and operations. Your Budget justification, including the status and plans for information systems, should be consistent with your agency's submissions for Part 7 (section 300) of this Circular.

The total investment's costs must cover the entire risk-adjusted life cycle of each system and include all budgetary resources (direct appropriation, working capital fund, revolving funds, etc.). Budgetary resources are defined in section 20 of this Circular. Life cycle costs should also be risk adjusted to include any risks addressed on the Capital Asset Plan and Business Case. These total investment costs must be formulated and reported in order for OMB to meet the Clinger-Cohen Act's requirement which states, at the same time the President submits the Budget for a fiscal year to Congress under Section 1105(a) of title 31, United States Code, the Director shall submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by executive agencies in information systems and how the benefits relate to the accomplishment of the goals of the executive agencies.

53.2 What background information must I know?

The Federal Government must effectively manage its portfolio of capital assets to ensure scarce public resources are wisely invested. Capital programming

integrates the planning, acquisition and management of capital assets into the Budget decision-making process. It is intended to assist agencies in improving asset management and in complying with the results-oriented requirements of:

• The Government Performance and Results Act of 1993 (GPRA), which establishes the foundation for Budget decision-making to achieve strategic goals in order to meet agency mission objectives. Instructions for preparing strategic plans, annual performance plans, and annual program performance reports are provided in Part 6 of this Circular (see section 220).

• The Program Assessment Rating Tool (PART), which assesses a program's performance and management, including the practices and procedures used to achieve results. Information on the PART process and schedule, guidance for completing a PART assessment, and other supporting materials can be found at http://www.whitehouse.gov/omb/part/.

• The Federal Managers Financial Integrity Act of 1982 (FMFIA), Chief Financial Officers Act of 1990 (CFO Act) and Federal Financial Management Improvement Act of 1996, which require accountability of financial and program managers for financial results of actions taken, control over the Federal Government's financial resources, and protection of Federal assets. OMB policies and standards for developing, operating, evaluating, and reporting on financial management systems are contained in Circular A–127, Financial Management Systems, and section 52 of this Circular.

• The Paperwork Reduction Act of 1995 (PRA), which requires agencies to perform their information resources management activities in an efficient, effective, and economical manner.

• The Clinger-Cohen Act of 1996, which requires agencies to use a disciplined capital planning and investment control (CPIC) process to acquire, use, maintain and dispose of information technology. OMB policy for management of Federal information resources is contained in Circular A–130, "Management of Federal Information Resources."

• The Federal Information Security Management Act (FISMA), which requires agencies to integrate IT security into their capital planning and enterprise architecture (EA) processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB.

• The E-Government Act of 2002 (P.L. 107–347), which requires agencies to support governmentwide E-Gov initiatives and to leverage cross-agency

opportunities to further E-Gov. The Act also requires agencies to establish a process for determining which government information the agency intends to make available and accessible to the public on the Internet and by other means. In addition, the Act requires agencies to conduct and make publicly available privacy impact assessments (PIAs) for all new IT investments administering information in identifiable form collected from or about members of the public.

• The National Technology Transfer and Advancement Act (NTTAA) of 1995 (Public Law 104- 113) and OMB Circular A-119, which state that voluntary consensus standards are the preferred type of standards for Federal government use. When it would be inconsistent with law or otherwise impractical to use a voluntary consensus standard, agencies must submit a report describing the reason(s) for the agency's use of government-unique standards in lieu of voluntary consensus standards to the Office of Management and Budget (OMB) through the National Institute of Standards and Technology (NIST).

• The Federal Records Act, which requires agencies to establish standards and procedures to assure efficient and effective records management. The National Archives and Records Administration (NARA) issues policies and guidance for agencies to meet their records management goals and requirements. NARA also provides policies and guidance for planning and evaluating investments in electronic records management.

• The Privacy Act (5 U.S.C. § 552a), is an omnibus "code of fair information practices" which attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies.

53.3 How do I ensure IT investments improve program performance and support the President's Management Agenda?

All IT investments must clearly demonstrate the investment is needed to help meet the agency's strategic goals and mission. They should also support the President's Management Agenda (PMA). The President's Budget defines the guiding principles for the investments supporting the PMA. For more information on the PMA refer to http://www.results.gov.

The capital asset plans and business cases (exhibit 300) and "Agency IT Investment Portfolio" (exhibit 53) demonstrate the agency management of IT investments and how these governance processes are used when planning and implementing IT investments within the agency. Any attendant documentation should be maintained and readily available if requested by OMB.

The individual agency's exhibit 53 is used to create an overall "Federal IT Investment Portfolio" published as part of the President's Budget. OMB's portfolio review and Budget process will ensure IT investments support the strategy identified in this section and ensure the Federal IT Investment Portfolio includes the most effective portfolio of investments to:

• Improve the management of programs to achieve better program outcomes;

• Ensure sound security of Federal information systems and appropriate protection of information held in those systems;

• Eliminate redundant or non productive IT investments through multi-agency collaboration;

• Support the Federal Enterprise Architecture (FEA);

• Support the Presidential initiatives and E-Gov strategy;

• Focus IT spending on high priority modernization initiatives;

• Manage major IT investments within 10% of cost, schedule, and performance objectives;

• Certify and accredit IT investments and systems; and

• Ensure privacy safeguards are implemented in electronic activities.

53.4 What special terms should I know?

Budget Execution represents activities associated with the legal and managerial uses of budgetary resources to achieve results that comply with the enacted Budget and Administration policy. Budget execution activities include but are not limited to: apportionments, allotments, commitments, reprogramming actions, incurring obligations, and funds control. See sections 120 through 150 of Part 4 of OMB Circular No. A-11 for a comprehensive list of Budget execution activities.

Budget Formulation represents activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop Budget priorities.

Business Reference Model (BRM) is a function-driven framework used to describe the lines of business and sub-functions performed by the Federal Government independent of the agencies performing them. IT investments are mapped to the BRM to identify collaboration opportunities.

Capital Planning and Investment Control (CPIC) means the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues.

Certification and Accreditation (C&A) is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.

Federal Enterprise Architecture (FEA) is a business-based framework for government-wide improvement. It describes the relationship between business functions and the technologies and information supporting them. The FEA is constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. For the next President's Budget, major IT investments should be aligned with each reference model within the FEA framework, except for the Data Reference Model. More information about the FEA reference models is available at http://www.egov.gov. The BRM and Service Component Reference Model (SRM) are briefly described in this section (53.4).

Financial Management consist of activities that support the interrelationships and interdependencies between budget, cost and management functions, and the information associated with business transactions.

Financial Operations represent activities associated with processing, recording, and reporting of revenues, receipts, disbursements, expenditures, assets, liabilities, and other financial transactions; reconciliation of asset and liability accounts, such as accounts or loans receivable, with subsidiary records and with external data, such as Treasury cash records; and preparing financial statements.

Financial Systems are comprised of one or more applications that are used for any of the following:

• Collecting, processing, maintaining, transmitting, and reporting data about financial events;
• Accumulating and reporting cost information; or
• Supporting the preparation of financial statements.

A financial system supports the processes necessary to record the financial consequences of events that occur as a result of business activities. Such events include information related to the receipt of appropriations or resources; acquisition of goods or services; payment or collections; recognition of guarantees, benefits to be provided, or other potential liabilities or other reportable activities.

Funding Source means the direct appropriation or other budgetary resources an agency receives. You need to identify the budget account and the budget authority provided. Report those budget accounts providing the financing for a particular investment. To avoid double counting, do not report any accounts receiving intragovernmental payments to purchase IT investments or services as funding sources.

Government Information means information created, collected, processed, disseminated, or disposed of by or for the Federal government.

High Risk Projects require special attention from oversight authorities and the highest levels of agency management because: 1) the agency has not consistently demonstrated the ability to manage complex projects; 2) of the exceptionally high development, operating, or maintenance costs, either in absolute terms or as a percentage of the agency's total IT portfolio; 3) it is being undertaken to correct recognized deficiencies in the adequate performance of an essential mission program or function of the agency, a component of the agency, or another organization, or 4) delay or failure would introduce for the first time inadequate performance or failure of an essential mission program or function of the agency, a component of the agency, or another organization. If a High Risk Project is represented by an entire IT Investment, the IT Investment would be also known as a High Risk Investment.

Information Resource Management (IRM) Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency's IRM strategic plan as required by 44 U.S.C. 3506(b)(2). IRM strategic plans should support the agency's strategic plan required in OMB Circular A–11, provide a description of how information resources management activities help accomplish agency missions, and ensure IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Information System means a discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated information technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Information Technology, as defined by the Clinger-Cohen Act of 1996, sections 5002, 5141, and 5142, means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is "used" by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

IT migration Investment means the partner agency's migration costs associated with moving an existing investment, system, process or capability to a Government-wide common solution. All IT E-Gov and

Line of Business (LoB) migration projects must be tracked separately and not part of a larger investment. As these projects almost always consist of activities with more than one agency, migration investments are "High Risk."

Major IT Investment means a system or an acquisition requiring special management attention because it: has significant importance to the mission or function of the agency, a component of the agency or another organization; is for financial management and obligates more than $500,000 annually; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency's capital planning and investment control process. OMB may work with the agency to declare other investments as major investments. If you are unsure about what invest-ments to consider as "major", consult your agency budget officer or OMB representative. Investments not considered "major" are "nonmajor."

Managing Partner represents the agency designated as the lead agency responsible for the implementation of the E-Gov or LoB initiative. The managing partner is also responsible for coordinating and submitting the exhibit 300 for the initiative and the exhibit 300 will be represented as part of the managing partner's budget portfolio.

New IT Project means an IT investment newly proposed by the agency that has not been previously funded by OMB. This does not include investments existing within the agency that have not previously been reported to OMB.

Non-Major IT Investment means any initiative or investment not meeting the definition of major defined above but is part of the agency's IT Portfolio. All non-major investments must be reported individually on the exhibit 53.

On-going IT Investment means an investment that has been through a complete Budget cycle with OMB and represents Budget decisions consistent with the President's Budget for the current year (BY–1).

Partner Agency represents the agency for an E-Gov or LoB initiative designated as an agency that should provide resources (e.g., funding, FTEs, in-kind) to the management, development, deployment, or maintenance of a common solution. The partner agency is also responsible for including the appropriate line items in its Exhibit 53 reflecting the amount of the contribution for each of the E-Gov or LoB initiatives to which it is providing resources.

Partner Agency IT "fee-for-service" represents the financial fees paid for by a partner agency for IT services provided.

Primary FEA Mapping is the identification of the primary function or service this IT investment supports. For the next President's Budget, investments should identify a primary mapping to either the BRM (Line of Business and associated sub-function) or to the SRM (Service Type and associated Component). Only one primary FEA mapping should be provided for each investment. A BRM mapping should be used if the investment primarily supports a functional area. If the investment primarily provides a service cross-cutting multiple functional areas, the SRM mapping should be provided. Guidance on the codes for the BRM and SRM primary mappings can be found at http://www.egov.gov. Note: BRM lines of business and sub-functions in the Mode of Delivery business area are not valid as primary FEA mappings.

Privacy Impact Assessment (PIA) is a process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. Consistent with September 26th, 2003 OMB guidance (M–03–22) implementing the privacy provisions of the E-Government Act, agencies must conduct and make publicly available PIAs for all new or significantly altered information technology investments administering information in identifiable form collected from or about members of the public.

Records includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included.

Segment Architecture Detailed results-oriented architecture (baseline and target) and a transition strategy for a portion or segment of the enterprise. Segments are individual elements of the enterprise describing core mission areas, and common or shared business services and enterprise services.

Service Component Reference Model (SRM) is a common framework and vocabulary used for characterizing the IT and business components collectively comprising an IT investment. The SRM helps agencies rapidly assemble IT solutions through the sharing and re-use of business and IT components. A component is a self-contained process, service, or IT capability with pre-determined functionality that may be exposed through a business or technology interface.

System of Records Notice (SORN) means a statement providing to the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

Validated E-Gov Standard means a private, voluntary or U.S. government-developed standard developed and adopted via a widely recognized and broadly accepted process. These standards have been validated for use by NIST. The E-Gov standard validation process and validated standards can be located at the NIST E-Gov Standards Resource Center.

53.5 How do I determine whether I must report?

Submit an agency IT investment portfolio (exhibit 53) to OMB if your government agency is subject to Executive Branch review (see Section 25.1).

53.6 How do I submit exhibit 53 and when is it due?

Section 53 requires the submission of exhibit 53 and PIAs. Additional attendant documents should be maintained and made available upon OMB request.

Initial draft of exhibit 53. In order for OMB and the agency to agree on what major investments and non-major investments will be reported for the next President's Budget process, OMB will be working with agencies to create initial draft exhibit 53 during the summer of 2008. Draft exhibit 53 should, at a minimum, include the unique IDs, investment title, and investment description. OMB will be providing additional information about these initial draft exhibit 53s.

You must submit an exhibit 53 in an electronic format, using a valid spreadsheet version, via the IT Budget submission system (https://max.omb.gov/itweb/itweb).

Your exhibit 53 is due to OMB by September 8, 2008, the exhibit 53 and all updates must be submitted via the IT Budget submission system (also known as ITWEB). In addition, you must update each exhibit 53 and the accompanying Capital Asset Plans and Business Cases (exhibit 300) to reflect any changes due to final budget decisions.

If agencies are requesting supplemental funds, which include changes to the agency's portfolio, as part of their supplemental request, agencies should submit an updated exhibit 53.

53.7 If I submitted exhibit 53 last year, how do I revise it this year?

If your agency submitted an exhibit 53 for the 2009 Budget, the appropriate information can be used to create the new worksheet using the provided FY 2010 template (submissions not compliant with the provided template will be rejected). Ongoing investments from FY 2009 to FY 2010, must include their corresponding FY 2009 Unique Project Identifiers (UPI) in the appropriate column of the Exhibit 53. It is important the file is updated to reflect PY for FY 2008, CY for FY 2009, and BY for FY 2010. The Exhibit 53 also requires MAX funding codes for all "Funding Sources" line items. Consistent with prior submissions, "Investment Descriptions" will be limited to 255 characters.

53.8 How is exhibit 53 organized?

(a) *Overview*.

As a general rule, exhibit 53 covers IT investments for your agency as a whole. Provide investment amounts in millions (provide up to six decimal points, at

least one decimal point is required) for PY through BY. Information reported here must be consistent with data you report in MAX schedule O, object classification (specifically, object classes 11.1 through 12.2, 23.1, 23.2, 25.2, 25.3, 25.7, 26.0, 31.0, and 41.0). Include all major IT investments, including financial management systems, reported in exhibit 300 as well as all migration, partner agency funding contribution, and non-major IT investments.

Exhibit 53 has six major parts:

• Part 1. IT investments for Mission Area Support.

• Part 2. IT investments for Infrastructure, Office Automation, and Telecommunications.

• Part 3. IT investments for Enterprise Architecture and Planning.

• Part 4. IT investments for Grants Management Systems.

• Part 5. Grants to State and Local IT Investments.

• Part 6. National Security Systems IT Investments.

All parts use the following common data elements (in order as they appear in the Exhibit 53):

• ***2009 Unique Project Identifier (UPI)*** means the unique project identifier used to report the investment in the 2009 Budget. Indicating the UPI used for the 2009 Budget process allows crosswalk and historical analysis crossing fiscal years for tracking purposes.

• ***2010 UPI*** means the identifier depicting agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, and two-digit investment category code. Details are provided in section 53.8.

• ***Investment Title*** means a definitive title explaining the investment. If the investment title has changed, include the previous name in parentheses. For "funding source" information, provide the 10- digit OMB max account code (OMB Circular A-11, Section 79.2). Additional information can be found in Part III of this circular.

• ***Investment Description*** means a short public description (limited to 255 characters) for each investment (major, migration, partner contribution, and non-major). This description should explain the entry item, its components, and what program(s) it supports. This description should be understandable to

someone who is not an expert of the agency. If the investment is part of a multi-agency initiative or part of another business case, please provide description of where that business case is located in the appropriate agency Budget submission (i.e. managing partner UPI). For example, if the investment represents your agency's participation in one of the Presidential initiatives, the description should state that this investment represents your agency's participation in one of the Presidential initiatives and should refer to the UPI of the managing partner's business case (i.e. managing partner UPI). For "funding source descriptions" please consult your OMB representative for specifics about what information should be included in this field

• ***Primary FEA Mapping - Line of Business or Service Type*** means the 3-digit code for either the primary Line of Business from the FEA BRM OR the primary cross-cutting Service Type from the FEA SRM. This is required for all investments. BRM Line of Business and SRM Type codes can be found at http://www.egov.gov. Note: The BRM Mode of Delivery lines of business are not valid for Primary FEA Mappings.

• ***Primary FEA Mapping - Sub-Function or Service Component*** means the 3-digit code for either the primary Sub-function under the BRM Line of Business OR the primary cross-cutting Service Component under the SRM Service Type identified in the BRM Line of Business or SRM Service Type. This is required for all investments. BRM Sub-functions and SRM components codes can be found at http://www.egov.gov. Note: The BRM Mode of Delivery sub functions are not valid for Primary FEA Mappings.

• ***Percentage Budget Formulation (BF)*** means an estimated percentage of the total IT investment budget authority associated with budget formulation.

• ***Percentage Budget Execution (BE)*** means an estimated percentage of the total IT investment budget authority associated with budget execution.

• ***Percentage Financial*** means an estimated percentage of the total IT investment budget authority associated with financial operations. See section 53.4 for a description. Exclude information about budget formulation and budget execution activities when determining this.

• ***Percentage Current Year (CY) and Budget Year (BY) IT Security*** means an estimated percentage of the total investment for each fiscal year associated with IT security for a specific investment. Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the agency's Inspector General. When determining the percentage IT security include the costs of:

• Risk assessment;
• Security planning and policy;
• Certification and accreditation;
• Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security);
• Authentication or cryptographic applications;
• Education, awareness, and training;
• System reviews/evaluations (including security control testing and evaluation);
• Oversight or compliance inspections;
• Development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment;
• Contingency planning and testing;
• Physical and environmental controls for hardware and software;
• Auditing and monitoring;
• Computer security investigations and forensics; and
• Reviews, inspections, audits and other evaluations performed on contractor facilities and operations.

Other than those costs included above, security costs may also include the products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security, systems administrator functions, and, for example, system upgrades within which new features obviate the need for other standalone security controls.

Many agencies operate networks, which provide some or all necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid double counting agencies should appropriately allocate the costs of the network for each of the applications for which security is provided. In identi-

fying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded. Therefore, if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the Budget materials.

• ***Percentage Internet Protocol version 6 (IPv6)*** means an estimated percentage of the total IT investment budget authority associated with the agency's IPv6 implementation.

• ***Homeland Security Presidential Directive-12 (HSPD-12)*** means the amount of this investment's PY/2008 funding associated with the agency's HSPD-12 implementation.

• ***Supports Homeland Security*** means an IT investment supporting the homeland security mission areas of 1) Intelligence and warning, 2) Border and transportation security, 3) Defending against catastrophic threats, 4) Protecting critical infrastructure and key assets, 5) Emergency preparedness and response, 6) Other. If the investment supports one of these mission areas, indicate which one(s) by listing the corresponding number(s) listed above. If the investment does not support homeland security, please leave blank.

• ***Development/Modernization/Enhancement (DME)*** means the program cost for new investments, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for investment management, and direct support. For major IT investments, this amount should equal the sum of amounts reported for planning and acquisition plus the associated FTE costs reported in the exhibit 300.

• ***Steady State (SS)*** means maintenance and operation costs at current capability and performance level including costs for personnel, maintenance of existing information systems, corrective software maintenance, voice and data communications maintenance, and replacement of broken IT equipment. For major IT investments, this amount should equal the amount reported for maintenance plus the associated FTE costs reported in the exhibit 300.

• ***Investment C&A status*** means the current security Certification and Accreditation (C&A) status of the investment's system(s):

(00)—Systems within this investment have not been through the C&A process because theinvestment is not yet operational.

(02)—None of the systems have gone through the C&A process or have been granted full authority to operate (for operational investments).

(22)—Some or all of the systems within this investment have been through a C&A process, but no systems have been granted full authority to operate.

(25)—Some or all of the systems within this investment have been through a C&A process, some systems have been granted full authority to operate.

(55)—All of the systems within this investment have been through a C&A process and have been granted full authority to operate.

• ***Project Management Qualification Status*** means the qualification status of the investment's project manager (PM), as issued in CIO Council Guidance and referenced by OMB PM Guidance (M–04–19). The following options are available:

(1)—The project manager assigned for this investment has been validated as qualified in accordance with OMB PM Guidance. (Validated PMs include "Validated with Exception".)

(2)—The project manager assigned for this investment is in the process of being validated as qualified in accordance with OMB PM Guidance.

(3)—The project manager assigned for this investment is not validated as qualified in accordance with OMB PM Guidance.

(4)—The qualifications for the project manager named have not been evaluated.

(5)—No project manager is currently assigned for this investment.

(6)—N/A—This is not an IT project/investment.

• ***On High-Risk List*** is to represent the projects/investments that are included on the agencies High Risk List.

• ***Segment Architecture*** represents the agency segment architecture the investment supports. The segment is identified by a unique code predetermined by the agency and the FEA PMO. The segment architecture code is a six digit code coordinated and maintained by the agency Chief Architect and registered with the FEA PMO. If new segments are established or revised, agencies are required to coordinate the numbering sequence with the FEA PMO office for approval. This is required for all investments. The agency Chief Architect should review the agency's portfolio to ensure accurate investment to segment architecture alignment. For detailed guidance regarding segment architecture codes, please refer to http://www.egov.gov.

• ***Funding Source*** means any budgetary resource used for funding the IT investment. Budgetary resource is defined in section 20. For each funding source, identify the budgetary resources including the MAX funding codes used for the investment. This is required for all investments. Add as many funding source line items as are appropriate for the investment. To avoid double

counting or under counting, the totals of the funding amounts for a investment must match the main investment line item, represented with the investment category of "00" or "24." Do not report funds received as part of intra-governmental payments to purchase IT investments or services, partner agencies should provide this as a part of the partner agency's IT portfolio.

• ***Funding Source Subtotal*** represents the total of all funding source line items used for funding a particular IT investment.

(b) *Part 1. IT investments for Mission Area Support.*

Consistent with your agency's strategic and annual performance plan, report amounts for IT investments directly supporting an agency-designated mission area (e.g., human resource management, financial management, command and control). Report each mission area in which IT investments are funded, itemizing the "major" and "non-major" IT investments within each mission area.

Agencies must have a mission area titled "Financial Management", and it must be reported as the first mission area. Some IT investments support financial functions in addition to other functions. If an IT investment supports financial functions, you must include an estimated percentage of the total IT investment obligations associated with the financial components. See the financial operations, budget formulation, and budget execution definitions provided in this section for a description of financial functions. For the purposes of this exhibit, the total investment for Financial Management is equal to the aggregated total of Budget Execution, Budget Formulations, and Financial Operations. Systems predominately supporting financial functions should be included in the first mission area, "Financial Management". If the IT investment reported is 100 percent financial, indicate "100" percent in the column. For mixed systems or investments, indicate the appropriate percentage that is financial.

(c) *Part 2. IT investments for Infrastructure, Office Automation, and Telecommunications.*

Report all IT investments supporting common user systems, communications, and computing infrastructure. Each agency should have one consolidated Exhibit 300

encompassing all office automation, infrastructure, and telecommunications for the agency. This investment usually involves multiple mission areas and includes End User Systems, Mainframes and Servers, and Telecommunications. The following descriptions will detail what should be included in Part – 2 of the Exhibit:

• ***End User Systems and Support*** - End user hardware (desktop, laptop, hand-held devices), peripherals (local printers, shared printers), and software (PC operating systems, office automation suites, messaging and groupware), and hardware and software for help desks.

• ***Mainframes and Servers Services and Support*** - Mainframes and servers [including web hosting (but not Web content development and management)], hardware and software operations, licenses, maintenance, back-up, continuity of operations, and disaster recovery. Also includes electronic messaging and storage.

• ***Telecommunications Systems and Support*** - Data networks and telecommunications (including wireless, multimedia, and local and long distance telephony) hardware and software operations, licenses, maintenance, back-up, continuity of operations, and disaster recovery. Also includes network operations command centers and wire closets and cable management.

If agencies have historically included additional activities in Part 2 of the Exhibit, the agency should specifically identify these activities in the consolidated Exhibit 300. The specific services should be provided in the Service Component Reference Model (SRM) Table.

Report your IT security initiatives and investments not directly tied to a major investment on a separate line identified as "non-major."

(d) *Part 3. IT investments for Enterprise Architecture and Planning.*

Report amounts for IT investments supporting strategic management of IT operations (e.g., business process redesign efforts not part of an individual investment or initiative, enterprise architecture development, capital planning and investment control processes, procurement management, and IT policy development and implementation).

(e) *Part 4. IT investments for Grants Management Systems.*

Report amounts for IT investments representing planning, developing, enhancing or implementing a grants management system or portion thereof. Include any grants systems initiatives.

(f) *Part 5. Grants to State and Local IT investments.*

Report amounts for IT investments representing planning, development, enhancements or implementations of "Grants to State and Local." Agencies should only use this part to report "Grants to State and Local." Before using Part 5 for anything other than the previously identified, please check with your OMB representative.

(g) *Part 6. National Security Systems investments.*

Report amounts for IT investments representing planning, development, enhancements or implementations of National Security Systems. Only DoD may use this part.

53.9 How is exhibit 53 coded?

Use the following 23 digit line number coding system to update or complete your exhibit 53:

Entry	**Description**
XXX–xx–xx–xx–xx–xxxx–xx	The first three digits are your agency code (see Appendix C).
xxx–XX–xx–xx–xx–xxxx–xx	The next two digits are your bureau code (see Appendix C). If this is a department only reporting, use 00 as your bureau code.
xxx–xx–XX–xx–xx–xxxx–xx	These two digits indicate the four parts of exhibit 53: 01 = Part 1. IT Investments by Mission Area 02 = Part 2. IT Investments for Infrastructure, Office Automation, and Telecommunications 03 = Part 3. IT Investments for Enterprise Architecture and Planning 04 = Part 4. IT Investments for Grants Management Systems 05 = Part 5. Grants to State and Locals 06 = Part 6. National Security Systems (Defense only)
xxx–xx–xx–XX–xx–xxxx–xx	These two digits indicate the mission area. Assign a unique code for each mission area reported.
xxx–xx–xx–xx–XX–xxxx–xx	These two digits indicate your agency's type of investment. Select one of the following two digit codes according to the type of investment you are reporting: 01 = Major IT investments (see definition in section 53.3) 02 = Non-major IT investments (see definition in section 53.3) 03= IT migration investment portion of a larger asset and for which there is an existing business case for the overall asset. Description of the IT investment should indicate the UPI of the

	major asset investment of the managing partner. 04 = Partner agency funding contribution represents resources provided by partner agency for a joint effort for more than one agency. Use the 04 indicator to identify projects where the business case for the major IT investment is reported in another agency's exhibit 53. Description of the IT investment should indicate the UPI of the major asset investment of the managing partner.
xxx–xx–xx–xx–xx–XXXX–xx	This is a four-digit identification number to identify a specific IT investment. If a new investment is added to exhibit 53, locate the area of exhibit 53 where you are going to report the IT investment and use the next sequential number as your four digit identification number.
xxx–xx–xx–xx–xx–xxxx–XX	These two digits identify the investment category of the investment you are reporting. Select one of the following two digit codes according to what you report on the title line: 00 = Total investment title line, or the first time the agency is reporting this particular investment. If this is one of the PMC E-Gov initiatives or an individual agency's participation in one of the PMC E-Gov initiatives, this two-digit code should be "24". 04 = Funding source or appropriation 07 = High-Risk Project as part of a larger investment (Migration projects may not use this code, these are defined by use of IT migration investment type) 09 = Any subtotal

Use the following 10 digit number coding system to update or complete your OMB MAX Account ID code information:

Entry	Description
XXX–xx–xxxx–x	The first three digits are your agency code (see Appendix C).
xxx–XX–xxxx–x	The next two digits are your bureau code (see Appendix C).

xxx–xx–XXXX-x	This is a four-digit Account Symbol for the appropriate MAX Account. (see section 79.2)
xxx–xx–xxxx-X	This is a single digit Transmittal Code. (see section 79.2)

53.10 What are the steps to complete exhibit 53?

The following provides step-by-step instructions to complete each part of exhibit 53. See section 53.3 and 53.7 for definitions.

AGENCY IT INVESTMENT PORTFOLIO

Entry	Description
Part 1. IT Investments by Mission Area	Report amounts (DME & SS) for IT investments that directly support an agency-designated mission area. Report each mission area in which IT investments are funded. This information should map directly to your agency's strategic and annual performance plan. For IT investments that cover more than one agency, report in the mission area with oversight of the IT investment. Mission area 01 is reserved for your "financial management" IT investments. **Step 1:** For each mission area, list each major IT investment and the corresponding investment costs. For BY only, if financial or mixed, identify what percentage is financial. For BY only, if IT security costs are included, identify what percentage of the total investment is IT security. If this IT investment supports Homeland Security (HS) goals and objectives (see section 53.8) provide the number for the HS mission area. **Step 2:** For each mission area, list each non-major investment. If either of these has financial, mixed, or IT security, identify the appropriate percentages. If this system or investment supports Homeland Security goals and objectives (see section 53.8), answer yes.

Part 2. IT investments for Infrastructure, Office Automation, and Telecommunications	Each agency should have one exhibit 300 encompassing all office automation, infrastructure, and telecommunications for the agency (see section 53.8). This section of the exhibit 53 should have one line item indicating the major investment Unique ID for this departmental/agency-wide investment. If you are unsure what investments should be included in this area contact your OMB representative for clarification. Additional information about the relationship between this consolidated business case and the Infrastructure LoB can be found at http://www.egov.gov
Part 3. IT Investments for Enterprise Architecture and Planning	Each agency should list all enterprise architecture efforts. For the next President's Budget, enterprise architecture investments are not categorized as major investments and an exhibit 300 is not required for them. Any capital planning and investment control process investments may be reported separately in this section. However, agencies should ensure the investments' UPI codes have the correct primary FEA mapping in order to clearly distinguish the EA investments from other planning investments (e.g., EA investments should be mapped to the "Enterprise Architecture" sub-function in the BRM).
Part 4. IT Investments for Grants Management Systems	Report amounts (DME & SS) for IT investments that support grants management operations. See classification instructions in section 53.8 under Grants Management.
Part 5. Grants to State and Local	Report amounts (DME & SS) for IT investments for Grants to State and Local.
Part 6. National Security Systems	Report amounts (DME & SS) for IT investments related to National Security Systems (Defense Only).

These columns are required for the next President's Budget exhibit 53, Agency IT Investment Portfolio:

Column 1: 2009 UPI (17-digits required for all legacy investments)
Column 2: 2010 UPI (17–digits required for all)
Column 3: Investment Title
Column 4: Investment Description (limited to 255 characters)
Column 5: Primary FEA Mapping - Line of Business or Service Type (3 digit code)
Column 6: Primary FEA Mapping - Sub-Function or Service Component (3 digit code)
Column 7: BF Percentage (%)
Column 8: BE Percentage (%)
Column 9: Financial Percentage (%)
Column 10: CY IT Security (%)
Column 11: BY IT Security (%)
Column 12: IPv6 (%)
Column 13: HSPD-12 ($M)
Column 14: Homeland Security Priority Identifier (select all that apply)
Column 15: Development, Modernization, Enhancement (DME) (PY/2008) ($M)
Column 16: Development, Modernization, Enhancement (DME) (CY/2009) ($M)
Column 17: Development, Modernization, Enhancement (DME) (BY/2010) ($M)
Column 18: Steady State (SS) (PY/2008) ($M)
Column 19: Steady State (SS) (CY/2009) ($M)
Column 20: Steady State (SS) (BY/2010) ($M)
Column 21: Investment C&A Status (00, 02, 22, 25, 55)
Column 22: Project Management Qualification Status (1, 2, 3, 4, 5, 6)
Column 23: On High-Risk List (Yes)
Column 24: Segment Architecture (6 digit code)

Deputy Secretary of Defense Memorandum: Designation of the Chief Information Officer of the Department of Defense

14 March 1996

THE DEPUTY SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

14 MAR 1996

C/6AC

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Designation of the Chief Information Officer of the Department of Defense

On February 10, 1996, the President signed the National Defense Authorization Act for Fiscal Year 1996. The Department strongly supports the requirements of this Act to establish both a Chief Information Officer (CIO) and a Deputy CIO and to implement management reforms that will institutionalize information technology performance measurements and results-based capital planning and investments.

Overall, the functions currently performed by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence are substantially identical to those of the proposed agency Chief Information Officer (CIO).

Therefore, effective immediately, in addition to their current duties, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) is designated as the CIO of the Department of Defense (DoD) and the Principal Deputy ASD(C3I) is designated as the Deputy CIO of the DoD. Further, within 150 days, CIOs will also be established in each of the Military Departments and Defense Agencies.

The ASD(C3I) will lead a joint DoD effort that will present within 150 days for my approval, coordinated procedures that implement the management requirements of Division E of the National Defense Authorization Act for Fiscal Year 1996, the Information Technology Management Reform Act of 1996.

U03078 96

10 U.S.C. Section 2223 - Information Technology: Additional Responsibilities of Chief Information Officers

U.S. Code	10 U.S.C. Subtitle A, PART IV, Chapter 131 § 2223
Date	Updated as of Jan. 3, 2007

(a) Additional Responsibilities of Chief Information Officer of Department of Defense.— In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of the Department of Defense shall—

(1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems;

(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;

(3) ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed;

(4) provide for the elimination of duplicate information technology and national security systems within and between the military departments and Defense Agencies; and

(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

(b) Additional Responsibilities of Chief Information Officer of Military Departments.— In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of a military department, with respect to the military department concerned, shall—

(1) review budget requests for all information technology and national security systems;

(2) ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense;

(3) ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and

(4) coordinate with the Joint Staff with respect to information technology and national security systems.

(c) Definitions.— In this section:

(1) The term "Chief Information Officer" means the senior official designated by the Secretary of Defense or a Secretary of a military department pursuant to section 3506 of title 44.

(2) The term "information technology" has the meaning given that term by section 11101 of title 40.

(3) The term "national security system" has the meaning given that term by section 3542 (b)(2) of title 44.

10 U.S.C. Section 2224 - Defense Information Assurance Program

U.S. Code	10 U.S.C. Subtitle A, PART IV, Chapter 131 § 2224
Date	Updated as of Jan. 3, 2007

(a) Defense Information Assurance Program.— The Secretary of Defense shall carry out a program, to be known as the "Defense Information Assurance Program", to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) Objectives of the Program.— The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) Program Strategy.— In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces.

(2) Development of essential information assurances technologies and programs.

(3) Organization of the Department, the armed forces, and supporting activities to defend against information warfare.

(4) Joint activities of the Department with other departments and agencies of the Government, State and local agencies, and elements of the national information infrastructure.

(5) The conduct of exercises, war games, simulations, experiments, and other activeties designed to prepare the Department to respond to information warfare threats.

(6) Development of proposed legislation that the Secretary considers necessary for implementing the program or for otherwise responding to the information warfare threat.

(d) Coordination.— In carrying out the program, the Secretary shall coordinate, as appropriate, with the head of any relevant Federal agency and with representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems.

[(e) Repealed. Pub. L. 108–136, div. A, title X, § 1031(a)(12), Nov. 24, 2003, 117 Stat. 1597.]

(f) Information Assurance Test Bed.— The Secretary shall develop an information assurance test bed within the Department of Defense to provide—

(1) an integrated organization structure to plan and facilitate the conduct of simulations, war games, exercises, experiments, and other activities to prepare and inform the Department regarding information warfare threats; and

(2) organization and planning means for the conduct by the Department of the integrated or joint exercises and experiments with elements of the national information systems infrastructure and other non-Department of Defense organizations that are responsible for the oversight and management of critical information systems and infrastructures on which the Department, the armed forces, and supporting activities depend for the conduct of daily operations and operations during crisis.

44 U.S.C. 3541-3549

Also known as Federal Information Security Management Act of 2002	
Date	Updated as of January 2, 2006.

SUBCHAPTER III--INFORMATION SECURITY

Federal Information Security Management Act of 2002

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Sec.

SUBCHAPTER III--INFORMATION SECURITY

Sec. 3541. Purposes

The purposes of this subchapter are to--

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

Sec. 3542. Definitions

(a) In General.--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) Additional Definitions.--As used in this subchapter

(1) The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(2)(A) The term `national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

(i) the function, operation, or use of which--

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(3) The term 'information technology' has the meaning given that term in section 11101 of title 40.

Sec. 3543. Authority and functions of the Director

(a) In General.--The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of--

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b);

(6) coordinating information security policies and procedures with related information resources management policies and procedures;

(7) overseeing the operation of the Federal information security incident center required under section 3546; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

(A) a summary of the findings of evaluations required by section 3545;

(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

(C) significant deficiencies in agency information security practices;

(D) planned remedial action to address such deficiencies; and

(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

(b) National Security Systems.--Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

(c) Department of Defense and Central Intelligence Agency Systems.--(1) The authorities of the Director described in paragraphs

(1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity

on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

Sec. 3544. Federal agency responsibilities

(a) In General.--The head of each agency shall—

(1) be responsible for— (A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40; and

(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and``

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including--

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agency wide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

(b) Agency Program.--Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or

destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with-

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for net-works, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

(B) may include testing relied on in a evaluation under section 3545;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—

(A) mitigating risks associated with such incidents before substantial damage is done;

(B) notifying and consulting with the Federal information security inci-dent center referred to in section 3546; and

(C) notifying and consulting with, as appropriate—

(i) law enforcement agencies and relevant Offices of Inspector General;

(ii) an office designated by the President for any incident involving a national security system; and

(iii) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) Agency Reporting.-- Each agency shall—

(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

(A) annual agency budgets;

(B) information resources management under subchapter 1 of this chapter;

(C) information technology management under subtitle III of title 40;

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

(G) internal accounting and administrative controls under section 3512 of title 31, (known as the 'Federal Managers Financial Integrity Act'); and

(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

(A) as a material weakness in reporting under section 3512 of title 31; and

(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

(d) Performance Plan.--(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods, and

(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

(e) Public Notice and Comment.--Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

Sec. 3545. Annual independent evaluation

(a) In General.--(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment (made on the basis of the results of the testing) of compliance with

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems

(b) Independent Auditor.--Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) National Security Systems.--For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) Existing Evaluations.--The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) Agency Reporting.--(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) Protection of Information.--Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB Reports to Congress.--(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems

in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) Comptroller General.--The Comptroller General shall periodically evaluate and report to Congress on—

(1) the adequacy and effectiveness of agency information security policies and practices; and

(2) implementation of the requirements of this subchapter.

Sec. 3546. Federal information security incident center

(a) In General.--The Director shall ensure the operation of a central Federal information security incident center to—

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security.

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) National Security Systems.--Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

Sec. 3547. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

Sec. 3548. Authorization of appropriations

There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

Sec. 3549. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.

44 U.S.C. 36 and Related Titles

Also known as the E Government Act of 2002	
Date	Updated as of January 2, 2006
Committee Reports	U.S. House Conference Report 107-787 U.S. House. Committee on Government Reform. H. Report No. 107-787, Part 1 accompanying H.R. 2458 U.S. Senate. Committee on Governmental Affairs.

E Government Act of 2002 Index

1. 44 U.S.C. Chapter 36

MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

Sec. 3601. Definitions

In this chapter, the definitions under section 3502 shall apply, and the term-

(1) Administrator means the Administrator of the Office of Electronic Government established under section 3602;

(2) Council means the Chief Information Officers Council established under section 3603; (3) electronic Government means the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to--

(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or

(B) bring about improvements in Government operations that may include effecttiveness, efficiency, service quality, or transformation;

(4) enterprise architecture--

(A) means

(i) a strategic information asset base, which defines the mission;

(ii) the information necessary to perform the mission;

(iii) the technologies necessary to perform the mission; and

(iv) the transitional processes for implementing new technologies in response to changing mission needs; and

(B) includes –

(i) a baseline architecture;

(ii) a target architecture; and

(iii) a sequencing plan;

(5) Fund means the E-Government Fund established under section 3604;

(6) interoperability means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner;

(7) integrated service delivery means the provision of Internet-based Federal Government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction; and

(8) tribal government means

(A) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and

(B) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.)

Sec. 3602. Office of Electronic Government

(a) There is established in the Office of Management and Budget an Office of Electronic Government.

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President

(c) The Administrator shall assist the Director in carrying out—

(1) all functions under this chapter;

(2) all of the functions assigned to the Director under title II of the E-Government Act of 2002; and

(3) other electronic government initiatives, consistent with other statutes.

(d) The Administrator shall assist the Director and the Deputy Director for Management and work with the Administrator of the Office of Information and Regulatory Affairs in setting strategic direction for implementing electronic Government, under relevant statutes, including-

(1) chapter 35;

(2) subtitle III of title 40, United States Code;

(3) section 552a of title 5 (commonly referred to as the Privacy Act);

(4) the Government Paperwork Elimination Act (44 U.S.C. 3504 note); and

(5) the Federal Information Security Management Act of 2002.

(e) The Administrator shall work with the Administrator of the Office of Information and Regulatory Affairs and with other offices within the Office of Management and Budget to oversee implementation of electronic Government under this chapter, chapter 35, the E-Government Act of 2002, and other relevant statutes, in a manner consistent with law, relating to--

(1) capital planning and investment control for information technology;

(2) the development of enterprise architectures;

(3) information security;

(4) privacy;

(5) access to, dissemination of, and preservation of Government information;

(6) accessibility of information technology for persons with disabilities; and

(7) other areas of electronic Government.

(f) Subject to requirements of this chapter, the Administrator shall assist the Director by performing electronic Government functions as follows:

(1) Advise the Director on the resources required to develop and effectively administer electronic Government initiatives.

(2) Recommend to the Director changes relating to Government-wide strategies and priorities for electronic Government.

(3) Provide overall leadership and direction to the executive branch on electronic Government.

(4) Promote innovative uses of information technology by agencies, particularly initiatives involving multiagency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies.

(5) Oversee the distribution of funds from, and ensure appropriate administration and coordination of, the E-Government Fund established under section 3604.

(6) Coordinate with the Administrator of General Services regarding programs undertaken by the General Services Administration to promote electronic government and the efficient use of information technologies by agencies.

(7) Lead the activities of the Chief Information Officers Council established under section 3603 on behalf of the Deputy Director for Management, who shall chair the council.

(8) Assist the Director in establishing policies which shall set the framework for information technology standards for the Federal Government developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce under section 11331 of title 40, taking into account, if appropriate, recommendations of the Chief Information Officers Council, experts, and interested parties from the private and nonprofit sectors and State, local, and tribal governments, and maximizing the use of commercial standards as appropriate, including the following:

(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.

(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.

(C) Standards and guidelines for Federal Government computer system efficiency and security.

(9) Sponsor ongoing dialogue that

(A) shall be conducted among Federal, State, local, and tribal government leaders on electronic Government in the executive, legislative, and judicial branches, as well as leaders in the private and nonprofit sectors, to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, using, and managing information resources;

(B) is intended to improve the performance of governments in collaborating on the use of information technology to improve the delivery of Government information and services; and

(C) may include

(i) development of innovative models

(I) for electronic Government management and Government information technology contracts; and

(II) that may be developed through focused discussions or using separately sponsored research;

(ii) identification of opportunities for public-private collaboration in using Internet-based technology to increase the efficiency of Government-to-business transactions;

(iii) identification of mechanisms for providing incentives to program managers and other Government employees to develop and implement innovative uses of information technologies; and

(iv) identification of opportunities for public, private, and intergovernmental collaboration in addressing the disparities in access to the Internet and information technology.

(10) Sponsor activities to engage the general public in the development and implementation of policies and programs, particularly activities aimed at fulfilling the goal of using the most effective citizen-centered strategies and those activities which engage multiple agencies providing similar or related information and services.

(11) Oversee the work of the General Services Administration and other agencies in developing the integrated Internet-based system under section 204 of the E-Government Act of 2002.

(12) Coordinate with the Administrator for Federal Procurement Policy to ensure effective implementation of electronic procurement initiatives.

(13) Assist Federal agencies, including the General Services Administration, the Department of Justice, and the United States Access Board in

(A) implementing accessibility standards under section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d); and

(B) ensuring compliance with those standards through the budget review process and other means.

(14) Oversee the development of enterprise architectures within and across agencies.

(15) Assist the Director and the Deputy Director for Management in overseeing agency efforts to ensure that electronic Government activities incorporate adequate, risk-based, and cost-effective security compatible with business processes.

(16) Administer the Office of Electronic Government established under this section.

(17) Assist the Director in preparing the E-Government report established under section 3606.

(g) The Director shall ensure that the Office of Management and Budget, including the Office of Electronic Government, the Office of Information and Regulatory Affairs, and other relevant offices, have adequate staff and resources to properly fulfill all functions under the E-Government Act of 2002.

Sec. 3603. Chief Information Officers Council

(a) There is established in the executive branch a Chief Information Officers Council.

(b) The members of the Council shall be as follows:

(1) The Deputy Director for Management of the Office of Management and Budget, who shall act as chairperson of the Council.

(2) The Administrator of the Office of Electronic Government.

(3) The Administrator of the Office of Information and Regulatory Affairs.

(4) The chief information officer of each agency described under section 901(b) of title 31.

(5) The chief information officer of the Central Intelligence Agency.

(6) The chief information officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief information officers have been designated for such departments under section 3506(a) (2) (B).

(7) Any other officer or employee of the United States designated by the chairperson.

(c)(1) The Administrator of the Office of Electronic Government shall lead the activities of the Council on behalf of the Deputy Director for Management.

(2)(A) The Vice Chairman of the Council shall be selected by the Council from among its members.

(B) The Vice Chairman shall serve a 1-year term, and may serve multiple terms.

(3) The Administrator of General Services shall provide administrative and other support for the Council

(d) The Council is designated the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources.

(e) In performing its duties, the Council shall consult regularly with representatives of State, local, and tribal governments.

(f) The Council shall perform functions that include the following:

(1) Develop recommendations for the Director on Government information resources management policies and requirements.

(2) Share experiences, ideas, best practices, and innovative approaches related to information resources management.

(3) Assist the Administrator in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.

(4) Promote the development and use of common performance measures for agency information resources management under this chapter and title II of the E-Government Act of 2002.

(5) Work as appropriate with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40, and maximize the use of commercial standards as appropriate, including the following:

(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.

(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government elec-

tronic information to enable efficient use of technologies, such as through the use of extensible markup language.

(C) Standards and guidelines for Federal Government computer system efficiency and security.

(6) Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management.

(7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

Sec. 3604. E-Government Fund

(a)(1) There is established in the Treasury of the United States the E-Government Fund.

(2) The Fund shall be administered by the Administrator of the General Services Administration to support projects approved by the Director, assisted by the Administrator of the Office of Electronic Government, that enable the Federal Government to expand its ability, through the development and implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically.

(3) Projects under this subsection may include efforts to

(A) make Federal Government information and services more readily available to members of the public (including individuals, businesses, grantees, and State and local governments);

(B) make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and

(C) enable Federal agencies to take advantage of information technology in sharing information and conducting transactions with each other and with State and local governments.

(b)(1) The Administrator shall

(A) establish procedures for accepting and reviewing proposals for funding;

(B) consult with interagency councils, including the Chief Information Officers Council, the Chief Financial Officers Council, and other interagency management councils, in establishing procedures and reviewing proposals; and

(C) assist the Director in coordinating resources that agencies receive from the Fund with other resources available to agencies for similar purposes.

(2) When reviewing proposals and managing the Fund, the Administrator shall observe and incorporate the following procedures:

(A) A project requiring substantial involvement or funding from an agency shall be approved by a senior official with agency wide authority on behalf of the head of the agency, who shall report directly to the head of the agency.

(B) Projects shall adhere to fundamental capital planning and investment con-trol processes.

(C) Agencies shall identify in their proposals resource commitments from the agencies involved and how these resources would be coordinated with sup-port from the Fund, and include plans for potential continuation of projects after all funds made available from the Fund are expended.

(D) After considering the recommendations of the interagency councils, the Director, assisted by the Administrator, shall have final authority to determine which of the candidate projects shall be funded from the Fund.

(E) Agencies shall assess the results of funded projects.

(c) In determining which proposals to recommend for funding, the Administrator

(1) shall consider criteria that include whether a proposal

(A) identifies the group to be served, including citizens, businesses, the Federal Government, or other governments;

(B) indicates what service or information the project will provide that meets needs of groups identified under subparagraph (A);

(C) ensures proper security and protects privacy;

(D) is interagency in scope, including projects implemented by a primary or single agency that—

(i) could confer benefits on multiple agencies; and

(ii) have the support of other agencies; and

(E) has performance objectives that tie to agency missions and strategic goals, and interim results that relate to the objectives; and

(2) may also rank proposals based on criteria that include whether a proposal

(A) has Governmentwide application or implications;

(B) has demonstrated support by the public to be served;

(C) integrates Federal with State, local, or tribal approaches to service delivery;

(D) identifies resource commitments from nongovernmental sectors;

(E) identifies resource commitments from the agencies involved;

(F) uses web-based technologies to achieve objectives;

(G) identifies records management and records access strategies;

(H) supports more effective citizen participation in and interaction with agency activities that further progress toward a more citizen-centered Government;

(I) directly delivers Government information and services to the public or provides the infrastructure for delivery;

(J) supports integrated service delivery;

(K) describes how business processes across agencies will reflect appropriate transformation simultaneous to technology implementation; and

(L) is new or innovative and does not supplant existing funding streams within agencies.

(d) The Fund may be used to fund the integrated Internet-based system under section 204 of the E-Government Act of 2002.

(e) None of the funds provided from the Fund may be transferred to any agency until 15 days after the Administrator of the General Services Administration has submitted to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and the appropriate authorizing committees of the Senate and the House of Representatives, a notification and description of how the funds are to be allocated and how the expenditure will further the purposes of this chapter.

(f)(1) The Director shall report annually to Congress on the operation of the Fund, through the report established under section 3606. (2) The report under paragraph (1) shall describe—

(A) all projects which the Director has approved for funding from the Fund; and

(B) the results that have been achieved to date for these funded projects.

(g)(1) There are authorized to be appropriated to the Fund--

(A) $45,000,000 for fiscal year 2003;

(B) $50,000,000 for fiscal year 2004;

(C) $100,000,000 for fiscal year 2005;

(D) $150,000,000 for fiscal year 2006; and

(E) such sums as are necessary for fiscal year 2007.

(2) Funds appropriated under this subsection shall remain available until expended.

Sec. 3605. Program to encourage innovative solutions to enhance electronic Government services and processes

(a) Establishment of Program.--The Administrator shall establish and promote a Governmentwide program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic Government services and processes.

(b) Issuance of Announcements Seeking Innovative Solutions.--Under the program, the Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall issue announcements seeking unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes.

(c) Multiagency Technical Assistance Team.--(1) The Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall convene a multiagency technical assistance team to assist in screening proposals submitted to the Administrator to provide unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes. The team shall be composed of employees of the agencies represented on the Council who have expertise in scientific and technical disciplines that would facilitate the assessment of the feasibility of the proposals.

(2) The technical assistance team shall—

(A) assess the feasibility, scientific and technical merits, and estimated cost of each proposal; and

(B) submit each proposal, and the assessment of the proposal, to the Administrator.

(3) The technical assistance team shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(4) After receiving proposals and assessments from the technical assistance team, the Administrator shall consider recommending appropriate proposals for funding

under the E-Government Fund established under section 3604 or, if appropriate, forward the proposal and the assessment of it to the executive agency whose mission most coincides with the subject matter of the proposal.

Sec. 3606. E-Government report

(a) Not later than March 1 of each year, the Director shall submit an E-Government status report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

(b) The report under subsection (a) shall contain—

(1) a summary of the information reported by agencies under section 202(f) of the E-Government Act of 2002;

(2) the information required to be reported by section 3604(f); and

(3) a description of compliance by the Federal Government with other goals and provisions of the E-Government Act of 2002.

2. 5 USC Chapter 37

INFORMATION TECHNOLOGY EXCHANGE PROGRAM

Sec. 3701. Definitions

For purposes of this chapter--

(1) the term 'agency' means an Executive agency, but does not include the General Accounting Office; and

(2) the term 'detail' means-

(A) the assignment or loan of an employee of an agency to a private sector organization without a change of position from the agency that employs the individual, or

(B) the assignment or loan of an employee of a private sector organization to an agency without a change of position from the private sector organization that

employs the individual, whichever is appropriate in the context in which such term is used.

Sec. 3702. General provisions

(a) Assignment Authority.--On request from or with the agreement of a private sector organization, and with the consent of the employee concerned, the head of an agency may arrange for the assignment of an employee of the agency to a private sector organization or an employee of a private sector organization to the agency. An eligible employee is an individual who—

(1) works in the field of information technology management;

(2) is considered an exceptional performer by the individual's current employer; and

(3) is expected to assume increased information technology management responsibilities in the future. An employee of an agency shall be eligible to participate in this program only if the employee is employed at the GS-11 level or above (or equivalent) and is serving under a career or career-conditional appointment or an appointment of equivalent tenure in the excepted service, and applicable requirements of section 209(b) of the E-Government Act of 2002 are met with respect to the proposed assignment of such employee.

(b) Agreements.--Each agency that exercises its authority under this chapter shall provide for a written agreement between the agency and the employee concerned regarding the terms and conditions of the employee's assignment. In the case of an employee of the agency, the agreement shall

(1) require the employee to serve in the civil service, upon completion of the assignment, for a period equal to the length of the assignment; and

(2) provide that, in the event the employee fails to carry out the agreement (except for good and sufficient reason, as determined by the head of the agency from which assigned) the employee shall be liable to the United States for payment of all expenses of the assignment. An amount under paragraph (2) shall be treated as a debt due the United States.

(c) Termination.--Assignments may be terminated by the agency or private sector organization concerned for any reason at any time.

(d) Duration.--Assignments under this chapter shall be for a period of between 3 months and 1 year, and may be extended in 3-month increments for a total of not more than 1 additional year, except that no assignment under this chapter may commence after the end of the 5- year period beginning on the date of the enactment of this chapter.

(e) Assistance.--The Chief Information Officers Council, by agreement with the Office of Personnel Management, may assist in the administration of this chapter, including by maintaining lists of potential candidates for assignment under this chapter, establishing mentoring relationships for the benefit of individuals who are given assignments under this chapter, and publicizing the program.

(f) Considerations.--In exercising any authority under this chapter, an agency shall take into consideration—

(1) the need to ensure that small business concerns are appropriately represented with respect to the assignments described in sections 3703 and 3704, respectively; and

(2) how assignments described in section 3703 might best be used to help meet the needs of the agency for the training of employees in information technology management.

Sec. 3703. Assignment of employees to private sector organizations

(a) In General.--An employee of an agency assigned to a private sector organization under this chapter is deemed, during the period of the assignment, to be on detail to a regular work assignment in his agency.

(b) Coordination With Chapter 81.--Notwithstanding any other provision of law, an employee of an agency assigned to a private sector organization under this chapter is entitled to retain coverage, rights, and benefits under subchapter I of chapter 81, and employment during the assignment is deemed employment by the United States, except that, if the employee or the employee's dependents receive from the private sector organization any payment under an insurance policy for which the premium is wholly paid by the private sector organization, or other benefit of any kind on account of the same injury or death, then, the amount of such payment or benefit shall be credited against any compensation otherwise payable under subchapter I of chapter 81.

(c) Reimbursements.--The assignment of an employee to a private sector organization under this chapter may be made with or without reimbursement by the private sector organization for the travel and transportation expenses to or from the place of assignment, subject to the same terms and conditions as apply with respect to an employee of a Federal agency or a State or local government under section 3375, and for the pay, or a part thereof, of the employee during assignment. Any reimbursements shall be credited to the appropriation of the agency used for paying the travel and transportation expenses or pay.

(d) Tort Liability; Supervision.--The Federal Tort Claims Act and any other Federal tort liability statute apply to an employee of an agency assigned to a private sector organization under this chapter. The supervision of the duties of an employee of an agency so assigned to a private sector organization may be governed by an agreement between the agency and the organization.

(e) Small Business Concerns.—

(1) In general.--The head of each agency shall take such actions as may be necessary to ensure that, of the assignments made under this chapter from such agency to private sector organizations in each year, at least 20 percent are to small business concerns.

(2) Definitions.--For purposes of this subsection—

(A) the term 'small business concern' means a business concern that satisfies the definitions and standards specified by the Administrator of the Small Business Administration under section 3(a)(2) of the Small Business Act (as from time to time amended by the Administrator);

(B) the term 'year' refers to the 12-month period beginning on the date of the enactment of this chapter, and each succeeding 12-month period in which any assignments under this chapter may be made; and

(C) the assignments 'made' in a year are those commencing in such year.

(3) Reporting requirement.--An agency which fails to comply with paragraph (1) in a year shall, within 90 days after the end of such year, submit a report to the Committees on Government Reform and Small Business of the House of Representatives and the Committees on Governmental Affairs and Small Business of the Senate. The report shall include—

(A) the total number of assignments made under this chapter from such agency to private sector organizations in the year;

(B) of that total number, the number (and percentage) made to small business concerns; and

(C) the reasons for the agency's noncompliance with paragraph (1).

(4) Exclusion.--This subsection shall not apply to an agency in any year in which it makes fewer than 5 assignments under this chapter to private sector organizations.

Sec. 3704. Assignment of employees from private sector organizations

(a) In General.--An employee of a private sector organization assigned to an agency under this chapter is deemed, during the period of the assignment, to be on detail to such agency.

(b) Terms and Conditions.--An employee of a private sector organization assigned to an agency under this chapter

(1) may continue to receive pay and benefits from the private sector organization from which he is assigned;

(2) is deemed, notwithstanding subsection (a), to be an employee of the agency for the purposes of—

(A) chapter 73;

(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18;

(C) sections 1343, 1344, and 1349(b) of title 31;

(D) the Federal Tort Claims Act and any other Federal tort liability statute;

(E) the Ethics in Government Act of 1978;

(F) section 1043 of the Internal Revenue Code of 1986; and

(G) section 27 of the Office of Federal Procurement Policy Act;

(3) may not have access to any trade secrets or to any other nonpublic information which is of commercial value to the private sector organization from which he is assigned; and

(4) is subject to such regulations as the President may prescribe. The supervision of an employee of a private sector organization assigned to an agency under this chapter may be governed by agreement between the agency and the private sector organization concerned. Such an assignment may be made with or without reimbursement by the agency for the pay, or a part there-of, of the employee during the period of assignment, or for any contribution of the private sector organization to employee benefit systems.

(c) Coordination With Chapter 81.--An employee of a private sector organization assigned to an agency under this chapter who suffers disability or dies as a result of personal injury sustained while performing duties during the assignment shall be treated, for the purpose of subchapter I of chapter 81, as an employee as defined by section 8101 who had sustained the injury in the performance of duty, except that, if the employee or the employee's dependents receive from the private sector organization any payment under an insurance policy for which the premium is wholly paid by the private sector organization, or other benefit of any kind on account of the same injury or death, then, the

amount of such payment or benefit shall be credited against any compensation otherwise payable under subchapter I of chapter 81.

(d) Prohibition Against Charging Certain Costs to the Federal Government.--A private sector organization may not charge the Federal Government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee assigned to an agency under this chapter for the period of the assignment.

Sec. 3705. Application to Office of the Chief Technology Officer of the District of Columbia

(a) In General.--The Chief Technology Officer of the District of Columbia may arrange for the assignment of an employee of the Office of the Chief Technology Officer to a private sector organization, or an employee of a private sector organization to such Office, in the same manner as the head of an agency under this chapter.

(b) Terms and Conditions.--An assignment made pursuant to subsection (a) shall be subject to the same terms and conditions as an assignment made by the head of an agency under this chapter, except that in applying such terms and conditions to an assignment made pursuant to subsection (a), any reference in this chapter to a provision of law or regulation of the United States shall be deemed to be a reference to the applicable provision of law or regulation of the District of Columbia, including the applicable provisions of the District of Columbia Government Comprehensive Merit Personnel Act of 1978 (sec. 1-601.01 et seq., D.C. Official Code) and section 601 of the District of Columbia Campaign Finance Reform and Conflict of Interest Act (sec. 1-1106.01, D.C. Official Code).

(c) Definition.--For purposes of this section, the term 'Office of the Chief Technology Officer' means the office established in the executive branch of the government of the District of Columbia under the Office of the Chief Technology Officer Establishment Act of 1998 (sec. 1-1401 et seq., D.C. Official Code).

Sec. 3706. Reporting requirement

(a) In General.--The Office of Personnel Management shall, not later than April 30 and October 31 of each year, prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a semiannual report summarizing the operation of this chapter during the immediately preceding 6-month period ending on March 31 and September 30, respectively.

(b) Content.--Each report shall include, with respect to the 6-month period to which such report relates—

(1) the total number of individuals assigned to, and the total number of individuals assigned from, each agency during such period;

(2) a brief description of each assignment included under paragraph

(1), including—

(A) the name of the assigned individual, as well as the private sector organization and the agency (including the specific bureau or other agency component) to or from which such individual was assigned;

(B) the respective positions to and from which the individual was assigned, including the duties and responsibilities and the pay grade or level associated with each; and

(C) the duration and objectives of the individual's assignment; and

(3) such other information as the Office considers appropriate.

(c) Publication.--A copy of each report submitted under subsection

(a)(1) Federal Register, publication shall be published in the Federal Register; and

(2) Public information shall be made publicly available on the Internet.

(d) Agency Cooperation.--On request of the Office, agencies shall furnish such information and reports as the Office may require in order to carry out this section.

Sec. 3707. Regulations

The Director of the Office of Personnel Management shall prescribe regulations for the administration of this chapter.

(2) Report.--Not later than 4 years after the date of the enactment of this Act, the General Accounting Office shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report on the operation of chapter 37 of title 5, United States Code (as added by this subsection). Such report shall include—

(A) an evaluation of the effectiveness of the program established by such chapter; and

(B) a recommendation as to whether such program should be continued (with or without modification) or allowed to lapse.

(3) Clerical Amendment.--The analysis for part III of title 5, United States Code, is amended by inserting after the item relating to chapter 35 the following:

3. 41 U.S.C. Chapter 4 § 266a – Share in Savings Contracts

(a) Authority to enter into share-in-savings contracts

(1) The head of an executive agency may enter into a share-in-savings contract for information technology (as defined in section 11101 (6) of title 40) in which the Government awards a contract to improve mission-related or administrative processes or to accelerate the achievement of its mission and share with the contractor in savings achieved through contract performance.

(2)(A) Except as provided in subparagraph (B), a share-in-savings contract shall be awarded for a period of not more than five years.

(B) A share-in-savings contract may be awarded for a period greater than five years, but not more than 10 years, if the head of the agency determines in writing prior to award of the contract that—

(i) the level of risk to be assumed and the investment to be undertaken by the contractor is likely to inhibit the government from obtaining the needed information technology competitively at a fair and reasonable price if the contract is limited in duration to a period of five years or less; and

(ii) usage of the information technology to be acquired is likely to continue for a period of time sufficient to generate reasonable benefit for the government.

(3) Contracts awarded pursuant to the authority of this section shall, to the maximum extent practicable, be performance-based contracts that identify objective outcomes and contain performance standards that will be used to measure achievement and milestones that must be met before payment is made.

(4) Contracts awarded pursuant to the authority of this section shall include a provision containing a quantifiable baseline that is to be the basis upon which a savings share ratio is established that governs the amount of payment a contractor is to receive under the contract. Before commencement of performance of such a contract, the senior procurement executive of the agency shall determine in writing that the terms of the provision are quantifiable and will likely yield value to the Government.

(5)(A) The head of the agency may retain savings realized through the use of a share-in-savings contract under this section that are in excess of the total amount of savings paid to the contractor under the contract, but may not retain any portion of such savings that is attributable to a decrease in the number of civilian employees of the Federal Government performing the function. Except as pro-

vided in subparagraph (B), savings shall be credited to the appropriation or fund against which charges were made to carry out the contract and shall be used for information technology.

(B) Amounts retained by the agency under this subsection shall—

(i) without further appropriation, remain available until expended; and

(ii) be applied first to fund any contingent liabilities associated with share-in-savings procurements that are not fully funded.

(b) Cancellation and termination

(1) If funds are not made available for the continuation of a share-in-savings contract entered into under this section in a subsequent fiscal year, the contract shall be canceled or terminated. The costs of cancellation or termination may be paid out of—

(A) appropriations available for the performance of the contract;

(B) appropriations available for acquisition of the information technology procured under the contract, and not otherwise obligated; or

(C) funds subsequently appropriated for payments of costs of cancellation or termination, subject to the limitations in paragraph (3).

(2) The amount payable in the event of cancellation or termination of a share-in-savings contract shall be negotiated with the contractor at the time the contract is entered into.

(3)(A) Subject to subparagraph (B), the head of an executive agency may enter into share-in-savings contracts under this section in any given fiscal year even if funds are not made specifically available for the full costs of cancellation or termination of the contract if funds are available and sufficient to make payments with respect to the first fiscal year of the contract and the following conditions are met regarding the funding of cancellation and termination liability:

(i) The amount of unfunded contingent liability for the contract does not exceed the lesser of—

(I) 25 percent of the estimated costs of a cancellation or termination; or

(II) $5,000,000.

(ii) Unfunded contingent liability in excess of $1,000,000 has been approved by the Director of the Office of Management and Budget or the Director's designee.

(B) The aggregate number of share-in-savings contracts that may be entered into under subparagraph (A) by all executive agencies to which this subchapter applies in a fiscal year may not exceed 5 in each of fiscal years 2003, 2004, and 2005.

(c) Definitions

In this section:

(1) The term “contractor” means a private entity that enters into a contract with an agency.

(2) The term “savings” means—

(A) monetary savings to an agency; or

(B) savings in time or other benefits realized by the agency, including enhanced revenues (other than enhanced revenues from the collection of fees, taxes, debts, claims, or other amounts owed the Federal Government).

(3) The term “share-in-savings contract” means a contract under which—

(A) a contractor provides solutions for—

(i) improving the agency’s mission-related or administrative processes; or

(ii) accelerating the achievement of agency missions; and

(B) the head of the agency pays the contractor an amount equal to a portion of the savings derived by the agency from—

(i) any improvements in mission-related or administrative processes that result from implementation of the solution; or

(ii) acceleration of achievement of agency missions.

(d) Termination

No share-in-savings contracts may be entered into under this section after September 30, 2005.

4. Pub. L. 107-347, Sec 202-215

SEC. 202. FEDERAL AGENCY RESPONSIBILITIES.

(a) In General.—The head of each agency shall be responsible for—

(1) complying with the requirements of this Act [see Tables for classification] (including the amendments made by this Act), the related information resource management policies and guidance established by the Director of the Office of Management and Budget, and the related information technology standards promulgated by the Secretary of Commerce;

(2) ensuring that the information resource management policies and guidance established under this Act by the Director, and the related information technology standards promulgated by the Secretary of Commerce are communicated promptly and effectively to all relevant officials within their agency; and

(3) supporting the efforts of the Director and the Administrator of the General Services Administration to develop, maintain, and promote an integrated Internet-based system of delivering Federal Government information and services to the public under section 204.

(b) Performance Integration.—

(1) Agencies shall develop performance measures that demonstrate how electronic government enables progress toward agency objectives, strategic goals, and statutory mandates.

(2) In measuring performance under this section, agencies shall rely on existing data collections to the extent practicable.

(3) Areas of performance measurement that agencies should consider include—

(A) customer service;

(B) agency productivity; and

(C) adoption of innovative information technology, including the appropriate use of commercial best practices.

(4) Agencies shall link their performance goals, as appropriate, to key groups, including citizens, businesses, and other governments, and to internal Federal Government operations.

(5) As appropriate, agencies shall work collectively in linking their performance goals to groups identified under paragraph (4) and shall use information technology in delivering Government information and services to those groups.

(c) Avoiding Diminished Access.—When promulgating policies and implementing programs regarding the provision of Government information and services over the Internet, agency heads shall consider the impact on persons without access to the Internet, and shall, to the extent practicable—

(1) ensure that the availability of Government information and services has not been diminished for individuals who lack access to the Internet; and

(2) pursue alternate modes of delivery that make Government information and services more accessible to individuals who do not own computers or lack access to the Internet.

(d) Accessibility to People With Disabilities.—All actions taken by Federal departments and agencies under this Act [see Tables for classification] shall be in compliance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

(e) Sponsored Activities.—Agencies shall sponsor activities that use information technology to engage the public in the development and implementation of policies and programs.

(f) Chief Information Officers.—The Chief Information Officer of each of the agencies designated under chapter 36 of title 44, United States Code (as added by this Act) shall be responsible for—

(1) participating in the functions of the Chief Information Officers Council; and

(2) monitoring the implementation, within their respective agencies, of information technology standards promulgated by the Secretary of Commerce, including common standards for interconnectivity and interoperability, categorization of Federal Government electronic information, and computer system efficiency and security.

(g) E-Government Status Report.—

(1) In general.—Each agency shall compile and submit to the Director an annual E-Government Status Report on—

(A) the status of the implementation by the agency of electronic government initiatives;

(B) compliance by the agency with this Act [see Tables for classification]; and

(C) how electronic Government initiatives of the agency improve performance in delivering programs to constituencies.

(2) Submission.—Each agency shall submit an annual report under this subsection—

(A) to the Director at such time and in such manner as the Director requires;

(B) consistent with related reporting requirements; and

(C) which addresses any section in this title relevant to that agency.

(h) Use of Technology.—Nothing in this Act [see Tables for classification] supersedes the responsibility of an agency to use or manage information technology to deliver Government information and services that fulfill the statutory mission and programs of the agency.

(i) National Security Systems.—

(1) Inapplicability.—Except as provided under paragraph (2), this title does not apply to national security systems as defined in section 11103 of title 40, United States Code.

(2) Applicability.—This section, section 203, and section 214 do apply to national security systems to the extent practicable and consistent with law.

SEC. 203. COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES.

(a) Purpose.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

(b) Electronic Signatures.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105–277; 112 Stat. 2681–749 through 2681–751) [44 U.S.C. 3504 note], each Executive agency (as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

(c) Authority for Electronic Signatures.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

(d) Authorization of Appropriations.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federal bridge certification authority for digital signature compatibility, and for other activities consistent with this section, $8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

SEC. 204. FEDERAL INTERNET PORTAL.

(a) In General.—

(1) Public access.—The Director shall work with the Administrator of the General Services Administration and other agencies to maintain and promote an integrated Internet-based system of providing the public with access to Government information and services.

(2) Criteria.—To the extent practicable, the integrated system shall be designed and operated according to the following criteria:

(A) The provision of Internet-based Government information and services directed to key groups, including citizens, business, and other governments, and integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction.

(B) An ongoing effort to ensure that Internet-based Government services relevant to a given citizen activity are available from a single point.

(C) Access to Federal Government information and services consolidated, as appropriate, with Internet-based information and services provided by State, local, and tribal governments.

(D) Access to Federal Government information held by 1 or more agencies shall be made available in a manner that protects privacy, consistent with law.

(b) Authorization of Appropriations.—There are authorized to be appropriated to the General Services Administration $15,000,000 for the maintenance, improvement, and promotion of the integrated Internet-based system for fiscal year 2003, and such sums as are necessary for fiscal years 2004 through 2007.

SEC. 205. FEDERAL COURTS.

(a) Individual Court Websites.—The Chief Justice of the United States, the chief judge of each circuit and district and of the Court of Federal Claims, and the chief bankruptcy judge of each district shall cause to be established and maintained, for the court of which the judge is chief justice or judge, a website that contains the following information or links to websites with the following information:

(1) Location and contact information for the courthouse, including the telephone numbers and contact names for the clerk's office and justices' or judges' chambers.

(2) Local rules and standing or general orders of the court.

(3) Individual rules, if in existence, of each justice or judge in that court.

(4) Access to docket information for each case.

(5) Access to the substance of all written opinions issued by the court, regardless of whether such opinions are to be published in the official court reporter, in a text searchable format.

(6) Access to documents filed with the courthouse in electronic form, to the extent provided under subsection (c).

(7) Any other information (including forms in a format that can be downloaded) that the court determines useful to the public.

(b) Maintenance of Data Online.—

(1) Update of information.—The information and rules on each website shall be updated regularly and kept reasonably current.

(2) Closed cases.—Electronic files and docket information for cases closed for more than 1 year are not required to be made available online, except all written opinions with a date of issuance after the effective date of this section [see Effective Date note set out under section 3601 of this title] shall remain available online.

(c) Electronic Filings.—

"(1) In general.—Except as provided under paragraph (2) or in the rules prescribed under paragraph (3), each court shall make any document that is filed electronically publicly available online. A court may convert any document that is filed in paper form to electronic form. To the extent such conversions are made, all such electronic versions of the document shall be made available online.

(2) Exceptions.—Documents that are filed that are not otherwise available to the public, such as documents filed under seal, shall not be made available online.

(3) Privacy and security concerns.—

(A)(i) The Supreme Court shall prescribe rules, in accordance with sections 2072 and 2075 of title 28, United States Code, to protect privacy and security concerns relating to electronic filing of documents and the public availability under this subsection of documents filed electronically or converted to electronic form.

(ii) Such rules shall provide to the extent practicable for uniform treatment of privacy and security issues throughout the Federal courts.

(iii) Such rules shall take into consideration best practices in Federal and State courts to protect private information or otherwise maintain necessary information security.

(iv) Except as provided in clause (v), to the extent that such rules provide for the redaction of certain categories of information in order to protect privacy and security concerns, such rules shall provide that a party that wishes to file an otherwise proper document containing such protected information may file an unredacted document under seal, which shall be retained by the court as part of the record, and which, at the discretion of the court and subject to any applicable rules issued in accordance with chapter 131 of title 28, United States Code, shall be either in lieu of, or in addition to, a redacted copy in the public file.

(v) Such rules may require the use of appropriate redacted identifiers in lieu of protected information described in clause (iv) in any pleading, motion, or other paper filed with the court (except with respect to a paper that is an exhibit or other evidentiary matter, or with respect to a reference list described in this subclause), or in any written discovery response—

(I) by authorizing the filing under seal, and permitting the amendment as of right under seal, of a reference list that—

(aa) identifies each item of unredacted protected information that the attorney or, if there is no attorney, the party, certifies is relevant to the case; and

(bb) specifies an appropriate redacted identifier that uniquely corresponds to each item of unredacted protected information listed; and

(II) by providing that all references in the case to the redacted identifiers in such reference list shall be construed, without more, to refer to the corresponding unredacted item of protected information.

(B)(i) Subject to clause (ii), the Judicial Conference of the United States may issue interim rules, and interpretive statements relating to the application of such rules, which conform to the requirements of this paragraph and which shall cease to have effect upon the effective date of the rules required under subparagraph (A).

(ii) Pending issuance of the rules required under subparagraph (A), any rule or order of any court, or of the Judicial Conference, providing for the redaction of certain categories of information in order to protect privacy and security concerns arising from electronic filing or electronic conversion shall comply with, and be construed in conformity with, subparagraph (A)(iv).

(C) Not later than 1 year after the rules prescribed under subparagraph (A) take effect, and every 2 years thereafter, the Judicial Conference shall submit to Congress a report on the adequacy of those rules to protect privacy and security.

(d) Dockets With Links to Documents.—The Judicial Conference of the United States shall explore the feasibility of technology to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket sheet of that case.

(e) Cost of Providing Electronic Docketing Information.—[Amended section 303(a) of Pub. L. 102–140, set out as a note under section 1913 of Title 28, Judiciary and Judicial Procedure.]

(f) Time Requirements.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the websites under

subsection (a) shall be established, except that access to documents filed in electronic form shall be established not later than 4 years after that effective date.

(g) Deferral.—

(1) In general.—

(A) Election.—

(i) Notification.—The Chief Justice of the United States, a chief judge, or chief bankruptcy judge may submit a notification to the Administrative Office of the United States Courts to defer compliance with any requirement of this section with respect to the Supreme Court, a court of appeals, district, or the bankruptcy court of a district.

(ii) Contents.—A notification submitted under this subparagraph shall state—

(I) the reasons for the deferral; and

(II) the online methods, if any, or any alternative methods, such court or district is using to provide greater public access to information.

(B) Exception.—To the extent that the Supreme Court, a court of appeals, district, or bankruptcy court of a district maintains a website under subsection (a), the Supreme Court or that court of appeals or district shall comply with subsection (b)(1).

(2) Report.—Not later than 1 year after the effective date of this title [see Effective Date note set out under section 3601 of this title], and every year thereafter, the Judicial Conference of the United States shall submit a report to the Committees on Governmental Affairs and the Judiciary of the Senate and the Committees on Government Reform and the Judiciary of the House of Representatives that—

(A) contains all notifications submitted to the Administrative Office of the United States Courts under this subsection; and

(B) summarizes and evaluates all notifications.

SEC. 206. REGULATORY AGENCIES.

(a) Purposes.—The purposes of this section are to—

(1) improve performance in the development and issuance of agency regulations by using information technology to increase access, accountability, and transparency; and

(2) enhance public participation in Government by electronic means, consistent with requirements under subchapter II of chapter 5 of title 5, United States Code, (commonly referred to as the ‘Administrative Procedures Act’).

(b) Information Provided by Agencies Online.—To the extent practicable as determined by the agency in consultation with the Director, each agency (as defined under section 551 of title 5, United States Code) shall ensure that a publicly accessible Federal Government website includes all information about that agency required to be published in the Federal Register under paragraphs (1) and (2) of section 552 (a) of title 5, United States Code.

(c) Submissions by Electronic Means.—To the extent practicable, agencies shall accept submissions under section 553 (c) of title 5, United States Code, by electronic means.

(d) Electronic Docketing.—

(1) In general.—To the extent practicable, as determined by the agency in consultation with the Director, agencies shall ensure that a publicly accessible Federal Government website contains electronic dockets for rulemakings under section 553 of title 5, United States Code.

(2) Information available.—Agency electronic dockets shall make publicly available online to the extent practicable, as determined by the agency in consultation with the Director—

(A) all submissions under section 553 (c) of title 5, United States Code; and

(B) other materials that by agency rule or practice are included in the rulemaking docket under section 553 (c) of title 5, United States Code, whether or not submitted electronically.

(e) Time Limitation.—Agencies shall implement the requirements of this section consistent with a timetable established by the Director and reported to Congress in the first annual report under section 3606 of title 44 (as added by this Act).

SEC. 207. ACCESSIBILITY, USABILITY, AND PRESERVATION OF GOVERNMENT INFORMATION.

(a) Purpose.—The purpose of this section is to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

(b) Definitions.—In this section, the term—

(1) ‘Committee’ means the Interagency Committee on Government Information established under subsection (c); and

(2) ‘directory’ means a taxonomy of subjects linked to websites that—

(A) organizes Government information on the Internet according to subject matter; and

(B) may be created with the participation of human editors.

(c) Interagency Committee.—

(1) Establishment.—Not later than 180 days after the date of enactment of this title [Dec. 17, 2002], the Director shall establish the Interagency Committee on Government Information.

(2) Membership.—The Committee shall be chaired by the Director or the designee of the Director and—

(A) shall include representatives from—

(i) the National Archives and Records Administration;

(ii) the offices of the Chief Information Officers from Federal agencies; and

(iii) other relevant officers from the executive branch; and

(B) may include representatives from the Federal legislative and judicial branches.

(3) Functions.—The Committee shall—

(A) engage in public consultation to the maximum extent feasible, including consultation with interested communities such as public advocacy organizations;

(B) conduct studies and submit recommendations, as provided under this section, to the Director and Congress; and

(C) share effective practices for access to, dissemination of, and retention of Federal information.

(4) Termination.—The Committee may be terminated on a date determined by the Director, except the Committee may not terminate before the Committee submits all recommendations required under this section.

(d) Categorizing of Information.—

(1) Committee functions.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director on—

(A) the adoption of standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

(i) in a way that is searchable electronically, including by searchable identifiers; and

(ii) in ways that are interoperable across agencies;

(B) the definition of categories of Government information which should be classified under the standards; and

(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

(2) Functions of the director.—Not later than 1 year after the submission of recommendations under paragraph (1), the Director shall issue policies—

(A) requiring that agencies use standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

(i) in a way that is searchable electronically, including by searchable identifiers;

(ii) in ways that are interoperable across agencies; and

(iii) that are, as appropriate, consistent with the provisions under section 3602 (f)(8) of title 44, United States Code;

(B) defining categories of Government information which shall be required to be classified under the standards; and

(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

(3) Modification of policies.—After the submission of agency reports under paragraph (4), the Director shall modify the policies, as needed, in consultation with the Committee and interested parties.

(4) Agency functions.—Each agency shall report annually to the Director, in the report established under section 202 (g), on compliance of that agency with the policies issued under paragraph (2)(A).

(e) Public Access to Electronic Information.—

(1) Committee functions.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director and the Archivist of the United States on—

(A) the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) the imposition of timetables for the implementation of the policies and procedures by agencies.

(2) Functions of the archivist.—Not later than 1 year after the submission of recommendations by the Committee under paragraph (1), the Archivist of the United States shall issue policies—

(A) requiring the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) imposing timetables for the implementation of the policies, procedures, and technologies by agencies.

(3) Modification of policies.—After the submission of agency reports under paragraph (4), the Archivist of the United States shall modify the policies, as needed, in consultation with the Committee and interested parties.

(4) Agency functions.—Each agency shall report annually to the Director, in the report established under section 202 (g), on compliance of that agency with the policies issued under paragraph (2)(A).

(f) Agency Websites.—

(1) Standards for agency websites.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director shall promulgate guidance for agency websites that includes—

(A) requirements that websites include direct links to—

(i) descriptions of the mission and statutory authority of the agency;

(ii) information made available to the public under subsections (a)(1) and (b) of section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act');

(iii) information about the organizational structure of the agency; and

(iv) the strategic plan of the agency developed under section 306 of title 5, United States Code; and

(B) minimum agency goals to assist public users to navigate agency websites, including—

(i) speed of retrieval of search results;

(ii) the relevance of the results;

(iii) tools to aggregate and disaggregate data; and

(iv) security protocols to protect information.

(2) Agency requirements.—(A) Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], each agency shall—

(i) consult with the Committee and solicit public comment;

(ii) establish a process for determining which Government information the agency intends to make available and accessible to the public on the Internet and by other means;

(iii) develop priorities and schedules for making Government information available and accessible;

(iv) make such final determinations, priorities, and schedules available for public comment;

(v) post such final determinations, priorities, and schedules on the Internet; and

(vi) submit such final determinations, priorities, and schedules to the Director, in the report established under section 202 (g).

(B) Each agency shall update determinations, priorities, and schedules of the agency, as needed, after consulting with the Committee and soliciting public comment, if appropriate.

(3) Public domain directory of public federal government websites.—

(A) Establishment.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director and each agency shall—

(i) develop and establish a public domain directory of public Federal Government websites; and

(ii) post the directory on the Internet with a link to the integrated Internet-based system established under section 204.

(B) Development.—With the assistance of each agency, the Director shall—

(i) direct the development of the directory through a collaborative effort, including input from—

(I) agency librarians; (II) information technology managers; (III) program managers; (IV) records managers; (V) Federal depository librarians; and (VI) other interested parties; and

(ii) develop a public domain taxonomy of subjects used to review and categorize public Federal Government websites.

(C) Update.—With the assistance of each agency, the Administrator of the Office of Electronic Government shall—

(i) update the directory as necessary, but not less than every 6 months; and

(ii) solicit interested persons for improvements to the directory.

(g) Access to Federally Funded Research and Development.—

(1) Development and maintenance of governmentwide repository and Website.—

(A) Repository and website.—The Director of the Office of Management and Budget (or the Director's delegate), in consultation with the Director of the Office of Science and Technology Policy and other relevant agencies, shall ensure the development and maintenance of—

(i) a repository that fully integrates, to the maximum extent feasible, information about research and development funded by the Federal Government, and the repository shall—

(I) include information about research and development funded by the Federal Government, consistent with any relevant protections for the information under section 552 of title 5, United States Code, and performed by—

(aa) institutions not a part of the Federal Government, including State, local, and foreign governments; industrial firms; educational institutions; not-for-profit organizations; federally funded research and development centers; and private individuals; and

(bb) entities of the Federal Government, including research and development laboratories, centers, and offices; and

(II) integrate information about each separate research and development task or award, including—

(aa) the dates upon which the task or award is expected to start and end;

(bb) a brief summary describing the objective and the scientific and technical focus of the task or award;

(cc) the entity or institution performing the task or award and its contact information;

(dd) the total amount of Federal funds expected to be provided to the task or award over its lifetime and the amount of funds expected to be provided in each fiscal year in which the work of the task or award is ongoing;

(ee) any restrictions attached to the task or award that would prevent the sharing with the general public of any or all of the information required by this subsection, and the reasons for such restrictions; and

(ff) such other information as may be determined to be appropriate; and

(ii) 1 or more websites upon which all or part of the repository of Federal research and development shall be made available to and searchable by Federal agencies and non-Federal entities, including the general public, to facilitate—

(I) the coordination of Federal research and development activities;

(II) collaboration among those conducting Federal research and development;

(III) the transfer of technology among Federal agencies and between Federal agencies and non-Federal entities; and

(IV) access by policymakers and the public to information concerning Federal research and development activities.

(B) Oversight.—The Director of the Office of Management and Budget shall issue any guidance determined necessary to ensure that agencies provide all information requested under this subsection.

(2) Agency functions.—Any agency that funds Federal research and development under this subsection shall provide the information required to populate the repository in the manner prescribed by the Director of the Office of Management and Budget.

(3) Committee functions.—Not later than 18 months after the date of enactment of this Act [Dec. 17, 2002], working with the Director of the Office of Science and Technology Policy, and after consultation with interested parties, the Committee shall submit recommendations to the Director on—

(A) policies to improve agency reporting of information for the repository established under this subsection; and

(B) policies to improve dissemination of the results of research performed by Federal agencies and federally funded research and development centers.

(4) Functions of the director.—After submission of recommendations by the Committee under paragraph (3), the Director shall report on the recommendations of the Committee and Director to Congress, in the E-Government report under section 3606 of title 44 (as added by this Act).

(5) Authorization of appropriations.—There are authorized to be appropriated for the development, maintenance, and operation of the Governmentwide repository and website under this subsection—

(A) $2,000,000 in each of the fiscal years 2003 through 2005; and

(B) such sums as are necessary in each of the fiscal years 2006 and 2007.

SEC. 208. PRIVACY PROVISIONS.

(a) Purpose.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) Privacy Impact Assessments.—

(1) Responsibilities of agencies.—

(A) In general.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physi-cal or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) Agency activities.—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) Sensitive information.—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) Copy to director.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) Contents of a privacy impact assessment.—

(A) In general.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) Guidance.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

(ii) require that a privacy impact assessment address—

(I) what information is to be collected;

(II) why the information is being collected;

(III) the intended use of the agency of the information;

(IV) with whom the information will be shared;

(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(VI) how the information will be secured; and

(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

(3) Responsibilities of the director.—The Director shall—

(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) Privacy Protections on Agency Websites.—

(1) Privacy policies on websites.—

(A) Guidelines for notices.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) Contents.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

(i) what information is to be collected;

(ii) why the information is being collected;

(iii) the intended use of the agency of the information;

(iv) with whom the information will be shared;

(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(vi) how the information will be secured; and

(vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

(2) Privacy policies in machine-readable formats.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) Definition.—In this section, the term 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

SEC. 209. FEDERAL INFORMATION TECHNOLOGY WORKFORCE DEVELOPMENT.

(a) Purpose.—The purpose of this section is to improve the skills of the Federal workforce in using information technology to deliver Government information and services.

(b) Workforce Development.—

(1) In general.—In consultation with the Director of the Office of Management and Budget, the Chief Information Officers Council, and the Administrator of General Services, the Director of the Office of Personnel Management shall—

(A) analyze, on an ongoing basis, the personnel needs of the Federal Government related to information technology and information resource management;

(B) identify where current information technology and information resource management training do not satisfy the personnel needs described in subparagraph (A);

(C) oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs of the Federal Government related to information technology and information resource management; and

(D) assess the training of Federal employees in information technology disciplines in order to ensure that the information resource management needs of the Federal Government are addressed.

(2) Information technology training programs.—The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection. Such programs shall—

(A) have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved;

(B) be developed and applied according to rigorous standards; and

(C) be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards.

(3) Governmentwide policies and evaluation.—The Director of the Office of Personnel Management, in coordination with the Director of the Office of Management and Budget, shall issue policies to promote the development of performance standards for training and uniform implementation of this subsection by Executive agencies, with due regard for differences in program requirements among agencies that may be appropriate and warranted in view of the agency mission. The Director of the Office of Personnel Management shall evaluate the implementation of the provisions of this subsection by Executive agencies.

(4) Chief information officer authorities and responsibilities.—Subject to the authority, direction, and control of the head of an Executive agency, the chief information officer of such agency shall carry out all powers, functions, and duties of the head of the agency with respect to implementation of this subsection. The chief information officer shall ensure that the policies of the agency head established in accordance with this subsection are implemented throughout the agency.

(5) Information technology training reporting.—The Director of the Office of Management and Budget shall ensure that the heads of Executive agencies collect and maintain standardized information on the information technology and information resources management workforce related to the implementation of this subsection.

(6) Authority to detail employees to non-Federal employers.—In carrying out the preceding provisions of this subsection, the Director of the Office of Person-

nel Management may provide for a program under which a Federal employee may be detailed to a non-Federal employer. The Director of the Office of Personnel Management shall prescribe regulations for such program, including the conditions for service and duties as the Director considers necessary.

(7) Coordination provision.—An assignment described in section 3703 of title 5, United States Code, may not be made unless a program under paragraph (6) is established, and the assignment is made in accordance with the requirements of such program.

(8) Employee participation.—Subject to information resource management needs and the limitations imposed by resource needs in other occupational areas, and consistent with their overall workforce development strategies, agencies shall encourage employees to participate in occupational information technology training.

(9) Authorization of Appropriations.—There are authorized to be appropriated to the Office of Personnel Management for the implementation of this subsection, $15,000,000 in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

(10) Executive agency defined.—For purposes of this subsection, the term 'Executive agency' has the meaning given the term 'agency' under section 3701 of title 5, United States Code (as added by subsection (c)).

(c) Information Technology Exchange Program.—

(1) In general.—[Enacted chapter 37 of Title 5, Government Organization and Employees.]

(2) Report.—Not later than 4 years after the date of the enactment of this Act [Dec. 17, 2002], the Government Accountability Office shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report on the operation of chapter 37 of title 5, United States Code (as added by this subsection). Such report shall include—

(A) an evaluation of the effectiveness of the program established by such chapter; and

(B) a recommendation as to whether such program should be continued (with or without modification) or allowed to lapse.

(3) Clerical Amendment.—[Amended analysis for part III of Title 5.]

(d) Ethics Provisions.—

(1) One-year restriction on certain communications.—[Amended section 207 of Title 18, Crimes and Criminal Procedure.]

(2) Disclosure of confidential information.—[Amended section 1905 of Title 18.]

(3) Contract advice.—[Amended section 207 of Title 18.]

(4) Restriction on disclosure of procurement information.—[Amended section 423 of Title 41, Public Contracts.]

(e) Report on Existing Exchange Programs.—

(1) Exchange program defined.—For purposes of this subsection, the term 'exchange program' means an executive exchange program, the program under subchapter VI of chapter 33 of title 5, United States Code, and any other program which allows for—

(A) the assignment of employees of the Federal Government to non-Federal employers;

(B) the assignment of employees of non-Federal employers to the Federal Government; or

(C) both.

(2) Reporting requirement.—Not later than 1 year after the date of the enactment of this Act [Dec. 17, 2002], the Office of Personnel Management shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report identifying all existing exchange programs.

(3) Specific information.—The report shall, for each such program, include—

(A) a brief description of the program, including its size, eligibility requirements, and terms or conditions for participation;

(B) specific citation to the law or other authority under which the program is established;

(C) the names of persons to contact for more information, and how they may be reached; and

(D) any other information which the Office considers appropriate.

(f) Report on the Establishment of a Governmentwide Information Technology Training Program.—

(1) In general.—Not later January 1, 2003, the Office of Personnel Management, in consultation with the Chief Information Officers Council and the Administrator of General Services, shall review and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a written report on the following:

(A) The adequacy of any existing information technology training programs available to Federal employees on a Governmentwide basis.

(B)(i) If one or more such programs already exist, recommendations as to how they might be improved.

(ii) If no such program yet exists, recommendations as to how such a program might be designed and established.

(C) With respect to any recommendations under subparagraph (B), how the program under chapter 37 of title 5, United States Code, might be used to help carry them out.

(2) Cost estimate.—The report shall, for any recommended program (or improvements) under paragraph (1)(B), include the estimated costs associated with the implementation and operation of such program as so established (or estimated difference in costs of any such program as so improved).

(g) Technical and Conforming Amendments.—

(1) Amendments to title 5, united states code.—[Amended sections 3111, 4108, and 7353 of Title 5.]

(2) Amendment to title 18, united states code.—[Amended section 209 of Title 18.]

(3) Other amendments.—[Amended section 125(c)(1) of Pub. L. 100–238, set out as a note under section 8432 of Title 5.]

SEC. 210. SHARE-IN-SAVINGS INITIATIVES.

(a) Defense Contracts.—[Enacted section 2332 of Title 10, Armed Forces.]

(b) Other Contracts.—[Enacted section 266a of Title 41.]

(c) Development of Incentives.—The Director of the Office of Management and Budget shall, in consultation with the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Sen-

ate, the Committee on Government Reform of the House of Representatives, and executive agencies, develop techniques to permit an executive agency to retain a portion of the savings (after payment of the contractor's share of the savings) derived from share-in-savings contracts as funds are appropriated to the agency in future fiscal years.

(d) Regulations.—Not later than 270 days after the date of the enactment of this Act [Dec. 17, 2002], the Federal Acquisition Regulation shall be revised to implement the provisions enacted by this section. Such revisions shall—

(1) provide for the use of competitive procedures in the selection and award of share-in-savings contracts to—

(A) ensure the contractor's share of savings reflects the risk involved and market conditions; and

(B) otherwise yield greatest value to the government; and

(2) allow appropriate regulatory flexibility to facilitate the use of share-in-savings contracts by executive agencies, including the use of innovative provisions for technology refreshment and nonstandard Federal Acquisition Regulation contract clauses.

(e) Additional Guidance.—The Administrator of General Services shall—

(1) identify potential opportunities for the use of share-in-savings contracts; and

(2) in consultation with the Director of the Office of Management and Budget, provide guidance to executive agencies for determining mutually beneficial savings share ratios and baselines from which savings may be measured.

(f) OMB Report to Congress.—In consultation with executive agencies, the Director of the Office of Management and Budget shall, not later than 2 years after the date of the enactment of this Act [Dec. 17, 2002], submit to Congress a report containing—

(1) a description of the number of share-in-savings contracts entered into by each executive agency under by [sic] this section and the amendments made by this section, and, for each contract identified—

(A) the information technology acquired;

(B) the total amount of payments made to the contractor; and

(C) the total amount of savings or other measurable benefits realized;

(2) a description of the ability of agencies to determine the baseline costs of a project against which savings can be measured; and

(3) any recommendations, as the Director deems appropriate, regarding additional changes in law that may be necessary to ensure effective use of share-in-savings contracts by executive agencies.

(g) GAO Report to Congress.—The Comptroller General shall, not later than 6 months after the report required under subsection (f) is submitted to Congress, conduct a review of that report and submit to Congress a report containing—

(1) the results of the review;

(2) an independent assessment by the Comptroller General of the effectiveness of the use of share-in-savings contracts in improving the mission-related and administrative processes of the executive agencies and the achievement of agency missions; and

(3) a recommendation on whether the authority to enter into share-in-savings contracts should be continued.

(h) Repeal of Share-in-Savings Pilot Program.—

(1) Repeal.—[Repealed section 11521 of Title 40, Public Buildings, Property, and Works.]

(2) Conforming amendments to pilot program authority.—[Amended sections 11501 to 11505 of Title 40.]

(3) Additional conforming amendments.—[Redesignated 11522 of Title 40 as 11521 and amended headings and analysis.]

(i) Definitions.—In this section, the terms 'contractor', 'savings', and 'share-in-savings contract' have the meanings given those terms in section 317 of the Federal Property and Administrative Services Act of 1949 [41 U.S.C. 266a] (as added by subsection (b)).

SEC. 211. AUTHORIZATION FOR ACQUISITION OF INFORMATION TECHNOLOGY BY STATE AND LOCAL GOVERNMENTS THROUGH FEDERAL SUPPLY SCHEDULES.

(a) Authority To Use Certain Supply Schedules.—[Amended section 502 of Title 40.]

(b) Procedures.—Not later than 30 days after the date of the enactment of this Act [Dec. 17, 2002], the Administrator of General Services shall establish procedures to implement section 501 (c) of title 40, United States Code (as added by subsection (a)).

(c) Report.—Not later than December 31, 2004, the Administrator shall submit to the Committee on Government Reform of the House of Representatives and

the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report on the implementation and effects of the amendment made by subsection (a).

SEC. 212. INTEGRATED REPORTING STUDY AND PILOT PROJECTS.

(a) Purposes.—The purposes of this section are to—

(1) enhance the interoperability of Federal information systems;

(2) assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information; and

(3) enable any person to integrate and obtain similar information held by 1 or more agencies under 1 or more Federal requirements without violating the privacy rights of an individual.

(b) Definitions.—In this section, the term—

(1) 'agency' means an Executive agency as defined under section 105 of title 5, United States Code; and

(2) 'person' means any individual, trust, firm, joint stock company, corporation (including a government corporation), partnership, association, State, municipality, commission, political subdivision of a State, interstate body, or agency or component of the Federal Government.

(c) Report.—

(1) In general.—Not later than 3 years after the date of enactment of this Act [Dec. 17, 2002], the Director shall oversee a study, in consultation with agencies, the regulated community, public interest organizations, and the public, and submit a report to the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate and the Committee on Government Reform of the House of Representatives on progress toward integrating Federal information systems across agencies.

(2) Contents.—The report under this section shall—

(A) address the integration of data elements used in the electronic collection of information within databases established under Federal statute without reducing the quality, accessibility, scope, or utility of the information contained in each database;

(B) address the feasibility of developing, or enabling the development of, software, including Internet-based tools, for use by reporting persons in assembling,

documenting, and validating the accuracy of information electronically submitted to agencies under nonvoluntary, statutory, and regulatory requirements;

(C) address the feasibility of developing a distributed information system involving, on a voluntary basis, at least 2 agencies, that—

(i) provides consistent, dependable, and timely public access to the information holdings of 1 or more agencies, or some portion of such holdings, without requiring public users to know which agency holds the information; and

(ii) allows the integration of public information held by the participating agencies;

(D) address the feasibility of incorporating other elements related to the purposes of this section at the discretion of the Director; and

(E) make any recommendations that the Director deems appropriate on the use of integrated reporting and information systems, to reduce the burden on reporting and strengthen public access to databases within and across agencies.

(d) Pilot Projects To Encourage Integrated Collection and Management of Data and Interoperability of Federal Information Systems.—

(1) In general.—In order to provide input to the study under subsection (c), the Director shall designate, in consultation with agencies, a series of no more than 5 pilot projects that integrate data elements. The Director shall consult with agencies, the regulated community, public interest organizations, and the public on the implementation of the pilot projects.

(2) Goals of pilot projects.—

(A) In general.—Each goal described under subparagraph (B) shall be addressed by at least 1 pilot project each.

(B) Goals.—The goals under this paragraph are to—

(i) reduce information collection burdens by eliminating duplicative data elements within 2 or more reporting requirements;

(ii) create interoperability between or among public databases managed by 2 or more agencies using technologies and techniques that facilitate public access; and

(iii) develop, or enable the development of, software to reduce errors in electronically submitted information.

(3) Input.—Each pilot project shall seek input from users on the utility of the pilot project and areas for improvement. To the extent practicable, the Director

shall consult with relevant agencies and State, tribal, and local governments in carrying out the report and pilot projects under this section.

(e) Protections.—The activities authorized under this section shall afford protections for—

(1) confidential business information consistent with section 552 (b)(4) of title 5, United States Code, and other relevant law;

(2) personal privacy information under sections 552 (b)(6) and (7)(C) and 552a of title 5, United States Code, and other relevant law;

(3) other information consistent with section 552 (b)(3) of title 5, United States Code, and other relevant law; and

(4) confidential statistical information collected under a confidentiality pledge, solely for statistical purposes, consistent with the Office of Management and Budget's Federal Statistical Confidentiality Order, and other relevant law.

SEC. 213. COMMUNITY TECHNOLOGY CENTERS.

(a) Purposes.—The purposes of this section are to—

(1) study and enhance the effectiveness of community technology centers, public libraries, and other institutions that provide computer and Internet access to the public; and

(2) promote awareness of the availability of on-line government information and services, to users of community technology centers, public libraries, and other public facilities that provide access to computer technology and Internet access to the public.

(b) Study and Report.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Administrator shall—

(1) ensure that a study is conducted to evaluate the best practices of community technology centers that have received Federal funds; and

(2) submit a report on the study to—

(A) the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate;

(B) the Committee on Health, Education, Labor, and Pensions of the Senate;

(C) the Committee on Government Reform of the House of Representatives; and

(D) the Committee on Education and the Workforce of the House of Representatives.

(c) Contents.—The report under subsection (b) may consider—

(1) an evaluation of the best practices being used by successful community technology centers;

(2) a strategy for—

(A) continuing the evaluation of best practices used by community technology centers; and

(B) establishing a network to share information and resources as community technology centers evolve;

(3) the identification of methods to expand the use of best practices to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public;

(4) a database of all community technology centers that have received Federal funds, including—

(A) each center's name, location, services provided, director, other points of contact, number of individuals served; and

(B) other relevant information;

(5) an analysis of whether community technology centers have been deployed effectively in urban and rural areas throughout the Nation; and

(6) recommendations of how to—

(A) enhance the development of community technology centers; and

(B) establish a network to share information and resources.

(d) Cooperation.—All agencies that fund community technology centers shall provide to the Administrator any information and assistance necessary for the completion of the study and the report under this section.

(e) Assistance.—

(1) In general.—The Administrator, in consultation with the Secretary of Education, shall work with other relevant Federal agencies, and other interested persons in the private and nonprofit sectors to—

(A) assist in the implementation of recommendations; and

(B) identify other ways to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public.

(2) Types of assistance.—Assistance under this subsection may include—

(A) contribution of funds;

(B) donations of equipment, and training in the use and maintenance of the equipment; and

(C) the provision of basic instruction or training material in computer skills and Internet usage.

(f) Online Tutorial.—

(1) In general.—The Administrator, in consultation with the Secretary of Education, the Director of the Institute of Museum and Library Services, other relevant agencies, and the public, shall develop an online tutorial that—

(A) explains how to access Government information and services on the Internet; and

(B) provides a guide to available online resources.

(2) Distribution.—The Administrator, with assistance from the Secretary of Education, shall distribute information on the tutorial to community technology centers, public libraries, and other institutions that afford Internet access to the public.

(g) Promotion of Community Technology Centers.—The Administrator, with assistance from the Department of Education and in consultation with other agencies and organizations, shall promote the availability of community technology centers to raise awareness within each community where such a center is located.

(h) Authorization of Appropriations.—There are authorized to be appropriated for the study of best practices at community technology centers, for the development and dissemination of the online tutorial, and for the promotion of community technology centers under this section—

(1) $2,000,000 in fiscal year 2003;

(2) $2,000,000 in fiscal year 2004; and

(3) such sums as are necessary in fiscal years 2005 through 2007.

SEC. 214. ENHANCING CRISIS MANAGEMENT THROUGH ADVANCED INFORMATION TECHNOLOGY.

(a) Purpose.—The purpose of this section is to improve how information technology is used in coordinating and facilitating information on disaster preparedness, response, and recovery, while ensuring the availability of such information across multiple access channels.

(b) In General.—

(1) Study on enhancement of crisis response.—Not later than 90 days after the date of enactment of this Act [Dec. 17, 2002], the Administrator, in consultation with the Federal Emergency Management Agency, shall ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.

(2) Contents.—The study under this subsection shall address—

(A) a research and implementation strategy for effective use of information technology in crisis response and consequence management, including the more effective use of technologies, management of information technology research initiatives, and incorporation of research advances into the information and communications systems of—

(i) the Federal Emergency Management Agency; and

(ii) other Federal, State, and local agencies responsible for crisis preparedness, response, and consequence management; and

(B) opportunities for research and development on enhanced technologies into areas of potential improvement as determined during the course of the study.

(3) Report.—Not later than 2 years after the date on which a contract is entered into under paragraph (1), the Administrator shall submit a report on the study, including findings and recommendations to—

(A) the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate; and

(B) the Committee on Government Reform of the House of Representatives.

(4) Interagency cooperation.—Other Federal departments and agencies with responsibility for disaster relief and emergency assistance shall fully cooperate with the Administrator in carrying out this section.

(5) Authorization of appropriations.—There are authorized to be appropriated for research under this subsection, such sums as are necessary for fiscal year 2003.

(c) Pilot Projects.—Based on the results of the research conducted under subsection (b), the Administrator, in consultation with the Federal Emergency Management Agency, shall initiate pilot projects or report to Congress on other activities that further the goal of maximizing the utility of information technology in disaster management. The Administrator shall cooperate with other relevant agencies, and, if appropriate, State, local, and tribal governments, in initiating such pilot projects.

SEC. 215. DISPARITIES IN ACCESS TO THE INTERNET.

(a) Study and Report.—

(1) Study.—Not later than 90 days after the date of enactment of this Act [Dec. 17, 2002], the Administrator of General Services shall request that the National Academy of Sciences, acting through the National Research Council, enter into a contract to conduct a study on disparities in Internet access for online Government services.

(2) Report.—Not later than 2 years after the date of enactment of this Act, the Administrator of General Services shall submit to the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate and the Committee on Government Reform of the House of Representatives a final report of the study under this section, which shall set forth the findings, conclusions, and recommendations of the National Research Council.

(b) Contents.—The report under subsection (a) shall include a study of—

(1) how disparities in Internet access influence the effectiveness of online Government services, including a review of—

(A) the nature of disparities in Internet access;

(B) the affordability of Internet service;

(C) the incidence of disparities among different groups within the population; and

(D) changes in the nature of personal and public Internet access that may alleviate or aggravate effective access to online Government services;

(2) how the increase in online Government services is influencing the disparities in Internet access and how technology development or diffusion trends may offset such adverse influences; and

(3) related societal effects arising from the interplay of disparities in Internet access and the increase in online Government services.

(c) Recommendations.—The report shall include recommendations on actions to ensure that online Government initiatives shall not have the unintended result of increasing any deficiency in public access to Government services.

(d) Authorization of Appropriations.—There are authorized to be appropriated $950,000 in fiscal year 2003 to carry out this section.

5. Pub. L. 101-508 title IV, § 4711(f)

Waiver of Paperwork Reduction Act

Pub. L. 101–508, title IV, § 4711(f), Nov. 5, 1990, 104 Stat. 1388–187, provided that: "Chapter 35 of title 44, United States Code, and Executive Order 12291 [formerly set out as a note under section 601 of Title 5, Government Organization and Employees] shall not apply to information and regulations required for purposes of carrying out this Act [see Tables for classification] and implementing the amendments made by this Act."

6. 44 U.S.C. Chapter 35 §3501 Notes

Source

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 163; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–217, § 3(l)(3), Aug. 21, 2002, 116 Stat. 1301.)

References in Text

Section 11332 of title 40, referred to in par. (8)(B), was repealed by Pub. L. 107–296, title X, § 1005(a)(1), Nov. 25, 2002, 116 Stat. 2272, and Pub. L. 107–347, title III, § 305(a), Dec. 17, 2002, 116 Stat. 2960.

Prior Provisions

A prior section 3501, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2812; amended Pub. L. 99–500, § 101(m) [title VIII, § 811], Oct. 18, 1986, 100 Stat. 1783–308, 1783–335, and Pub. L. 99–591, § 101(m) [title VIII, § 811], Oct. 30, 1986, 100 Stat. 3341–308, 3341–335, related to purposes of this chapter prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3501, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302, related to information for Federal agencies, prior to the general amendment of this chapter by Pub. L. 96–511.

Amendments

2002—Par. (8)(B). Pub. L. 107–217 substituted "section 11332 of title 40" for "the Computer Security Act of 1987 (Public Law 100–235)".

2000—Pub. L. 106–398 substituted "subchapter" for "chapter" in introductory provisions and in par. (11).

Effective Date of 2000 Amendment

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, set out as an Effective Date note under section 3531 of this title.

Effective Date

Section 4 of Pub. L. 104–13 provided that:

"(a) In General.—Except as otherwise provided in this section, this Act [enacting this chapter, amending section 91 of Title 13, Census, and enacting provisions set out as a note under section 101 of this title] and the amendments made by this Act shall take effect on October 1, 1995.

"(b) Authorization of Appropriations.—Section 3520 [now 3521] of title 44, United States Code, as amended by this Act, shall take effect on the date of enactment of this Act [May 22, 1995].

"(c) Delayed Application.—In the case of a collection of information for which there is in effect on September 30, 1995, a control number issued by the Office of Management and Budget under chapter 35 of title 44, United States Code—

"(1) the amendments made by this Act [enacting this chapter and amending section 91 of Title 13] shall apply to the collection of information beginning on the earlier of—

"(A) the first renewal or modification of that collection of information after September 30, 1995; or

"(B) the expiration of its control number after September 30, 1995.

"(2) prior to such renewal, modification, or expiration, the collection of information shall be subject to chapter 35 of title 44, United States Code, as in effect on September 30, 1995."

DoD Directive 5144.01

Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer (ASD(NII)/DoD CIO)

Date	May 2, 2005

References:
(a) Title 10, United States Code
(b) Title 44, United States Code
(c) Title 40, United States Code
(d) Unified Command Plan, March 1, 2005
(e) through (aa), see enclosure 1

1. PURPOSE

Under the authorities vested in the Secretary of Defense by section 113 of reference (a) and references (b) through (e), this Directive:

1.1. Assigns responsibilities, functions, relationships, and authorities to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO).

1.2. Cancels references (f) through (i).

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. RESPONSIBILITIES AND FUNCTIONS

The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT), including National Security Systems

(NSS); information resources management (IRM) (as defined by reference (b)); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C. (reference (j)), the ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective; Information and IT architect for the DoD enterprise; and, DoD-wide IT and IRM executive. Hereafter these responsibilities and functions are referred to collectively as "NII and CIO" (including IRM) matters. In the exercise of assigned responsibilities and functions, the ASD(NII)/DoD CIO shall:

3.1. Serve as the senior NII and CIO policy and resources official below the Secretary and Deputy Secretary of Defense.

3.2. Advise and assist the Secretary and Deputy Secretary of Defense on policy and issues regarding all assigned responsibilities and functions as they relate to the Department of Defense.

3.3. As the DoD CIO:

3.3.1. Review and provide recommendations to the Secretary and the Heads of the DoD Components on:

3.3.1.1. The performance of the Department's IT and NSS programs (to include monitoring and evaluating the performance of IT and NSS programs on the basis of all applicable performance measurements).

3.3.1.2. DoD budget requests for IT and NSS pursuant to section 2223 of reference (a).

3.3.1.3. The continuation, modification, or termination of an IT and/or NSS program or project pursuant to section 1425 of reference (c).

3.3.1.4. The continuation, modification, or termination of an NII or CIO program pursuant to the Federal Information Security Management Act of 2002 as part of Public Law (Pub. L.) 107-347 (reference (e)), Executive Order (E.O.). 13011 (reference (k)), and other applicable authorities.

3.3.2. Lead the formulation and implementation of enterprise-level defense strategies from the information, IT, network-centric, and non-intelligence space perspective.

3.3.3. Serve as the information architect for the DoD enterprise information environment, and provide oversight and policy guidance to ensure compliance with standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the Department, including intelligence systems and architectures. Ensure that IA is integrated into architectures pursuant to section 3534 of reference (b) and section 11315 of reference (c).

3.3.4. Perform the duties and fulfill the responsibilities associated with information security and other matters under section 3544 of reference (b).

3.3.5. Serve as the DoD-wide information executive and participate as a member on DoD-wide councils and boards involving NII and CIO matters, including serving as the DoD representative on the Intelligence Community CIO Executive Council.

3.3.6. Ensure that NII and CIO policy and resource decisions are fully responsive to the guidance of the Secretary and Deputy Secretary of Defense.

3.3.7. Develop and maintain the DoD IA program and associated policies, procedures, and standards required by section 2224 of reference (a), chapter 35 of reference (e) and DoD Directive S-3600.1 (reference (l)).

3.3.8. Ensure the interoperability of IT, including NSS, throughout the Department of Defense pursuant to section 2223 of reference (a).

3.3.9. Design and implement, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Under Secretary of Defense (Comptroller)/DoD Chief Financial Officer (USD(C)/CFO), the Under Secretary of Defense for Intelligence (USD(I)), and the Chairman of the Joint Chiefs of Staff, a process for maximizing the value and assessing and managing the risks of DoD IT acquisitions, including NSS acquisitions, as applicable.

3.3.10. Ensure compliance with the reduction of information-collection burdens on the public pursuant to section 3507 of reference (b).

3.3.11. Prescribe data and information management policies, procedures, and other guidance for the Department.

3.3.12. Issue policies and procedures necessary to establish and maintain a DoD Records Management Program pursuant to standards, guidelines, and procedures issued under section 2904 of reference (b) and Pub. L. No. 107-347 (reference (e)).

3.3.13. Ensure that IT, including NSS, standards that apply throughout the Department are prescribed and enforced pursuant to section 2223 of reference (a).

3.3.14. Provide advice and other assistance to the Secretary of Defense and other senior DoD managers to ensure that IT, including NSS, is acquired and information resources are managed in a manner consistent with reference (b) and section 11315 of reference (c) as well as the priorities established by the Secretary.

3.3.15. Provide enterprise-wide oversight of the development, integration, and implementation of the Global Information Grid (GIG) in accordance with DoD Directive 8100.1 (reference (m)).

3.3.16. Promote the effective and efficient design and operation of all major IRM processes, including improvements to work processes for the Department pursuant to section 11315 of reference (c).

3.3.17. Provide for the elimination of duplicate IT, including NSS, within and between the DoD Components, including the Military Departments and the Defense Agencies, pursuant to Section 2223 of reference (a).

3.3.18. Maintain a consolidated inventory of DoD mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems pursuant to section 2223 of reference (a).

3.3.19. Provide DoD-wide policy regarding the use of the Internet and Web site administration.

3.3.20. Develop policies, in coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), to provide oversight of training, career development, and occupation-specialty programs to ensure that personnel with the requisite knowledge and skills are available to support the DoD Information Enterprise.

3.3.21. Chair the DoD CIO Executive Board.

3.3.22. Establish policies, plans, goals, measures, and baselines to incorporate commercial-off-the-shelf software, knowledge management technologies, and services into the policies, doctrine, and training programs of the Department. Undertake initiatives to increase the use of commercial IT solutions throughout the Department across all applications, including NSS, training, logistics, and non-material solutions.

3.3.23. Serve as the principal DoD official responsible for preparing and defending NII and CIO issues before the Congress as well as evaluating and assessing Congressional activity for impact on all NII and CIO areas of responsibility.

3.3.24. Provide for the enterprise information environment and ensure that its capabilities are synchronized with requirements. This shall include providing for a common set of Enterprise capabilities that enable users to discover, access, post, process, advertise, retrieve, and fuse data, and make sense of the data gathered.

3.4. With regard to communications and information networks:

3.4.1. Develop and implement network-centric policies, architectures, practices, and processes with emphasis on communications and information networks to enable Defense transformation; however, these do not include content-based communications functions such as those associated with public affairs and public diplomacy.

3.4.2. Identify opportunities presented by communication and information technologies as well as risks and costs, and make recommendations on the initiation of communication and information plans, programs, policies, and procedures accordingly.

3.4.3. Provide policies, oversight, guidance, architecture, and strategic approaches for all communications and information network programs and initiatives on an enterprise-wide basis across the Department, ensuring compliance with the IA requirements as well as interoperability with national and alliance/coalition systems. This includes network-centric and information-integration projects, programs, and demonstrations as they relate to GIG implementation and employment.

3.4.4. Negotiate and conclude international agreements and other arrangements relating to the sharing or exchange of DoD communications equipment, facilities, support, services or other communications resources; the use of DoD electromagnetic spectrum equities; and the use of U.S. communications facilities and/or systems pursuant to DoD Directive 5530.3 (reference (n)). Agreements of an operational nature within alliance organizations shall be coordinated with the Chairman of the Joint Chiefs of Staff.

3.5. With regard to the electromagnetic spectrum:

3.5.1. Provide policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum, including the management and use of the electromagnetic spectrum (MUES) pursuant to DoD Directive 4650.1 (reference (o)) and the Electromagnetic Environmental Effects (E3) Program pursuant to DoD Directive 3222.3 (reference (p)) within the Department, nationally, and internationally. Ensure that appropriate national policies for MUES and E3 Control are implemented within the Department pursuant to section 305 and Chapter 8 of title 47, U.S.C. (reference (q)) and the National Telecommunications and Information Administration Manual (reference (r)) as well as applicable international policies and standards.

3.5.2. Serve as the lead within the Department for coordination, approval, and representation of DoD positions on all MUES and E3 Control matters with-in the U.S. Government as well as in regional, national, and international spectrum-management forums and organizations.

3.5.3. Coordinate, as appropriate, with the Chairman of the Joint Chiefs of Staff regarding the development of electromagnetic spectrum policy.

3.6. With regard to C2:

3.6.1. Develop and integrate the Department's overall C2 strategy, approach, structure, and policies and ensure the C2 structure and architecture are compliant with DoD network-centric precepts, information strategy, and joint needs.

3.6.2. Provide policies, program oversight, guidance, and strategic approaches for all C2 programs and initiatives on an enterprise-wide basis across the Department.

3.6.3. Identify the governance of the C2 structure that addresses the needs of the President and all levels of operational command within the Department.

3.6.4. Oversee and facilitate the integration of national, strategic, operational, and tactical C2 systems/programs, including support to the White House Military Office, pursuant to Secretary of Defense guidance (reference (s)).

3.6.5. Oversee the development and integration of DoD-wide C2 capabilities, including promotion of C2-related research, experimentation, metrics, and analysis techniques.

3.6.6. Direct the Heads of the DoD Components to plan, program, budget, and execute programs that will develop material solutions for Joint Capability Integration and Development System approved joint C2 capabilities.

3.7. With respect to space:

3.7.1. Oversee DoD non-intelligence related space matters, including space-based communications programs, space-based information integration activities, space control activities, operationally responsive space programs, space access, satellite control, space-based position, navigation, and timing programs, environmental sensing, and space launch ranges.

3.7.2. Oversee the Space Major Defense Acquisition Program activities of the DoD Executive Agent for Space in coordination with the USD(AT&L), and in coordination with the USD(I) for space-based intelligence system acquisitions, as delegated by the USD(AT&L).

3.8. With regard to network-centric systems engineering policy and program oversight:

3.8.1. Facilitate and resolve interoperability, performance, and other issues related to interfaces, security, standards, and protocols critical to the end-to-end operation of the GIG.

3.8.2. Oversee a network-centric system engineering effort using facilities and services of the Department of Defense to manage an enterprise-wide technical view for the GIG.

3.8.3. Provide oversight of policies and programs to support independent evaluation and to physically validate the technical performance for key transformational communication programs of the GIG.

3.9. With regard to systems acquisition:

3.9.1 Serve as the Milestone Decision Authority for Major Automated Information Systems and other acquisition programs, as delegated by the USD(AT&L), with responsibility for developing and enforcing the policies and practices of DoD Directive 5000.1 (reference (t)) for such programs, in coordination with the USD(AT&L) and the USD(I), as appropriate.

3.9.2. Provide advice on issues related to all assigned responsibilities and functions to the Defense Acquisition Board and the Defense Space Acquisition Board.

3.10. With regard to PNT:

3.10.1. Develop and implement PNT policy, including airspace and military air traffic control, pursuant to DoD Directive 4650.5 (reference (u)).

3.10.2. Develop and oversee contingency policies regarding the Federal Aviation Administration and its transfer to the Department of Defense under certain national security emergencies, pursuant to E.O. 11161 (reference (v)).

3.11. Support the Special Assistant to the Secretary of Defense and Deputy Secretary of Defense for compartmented activities by coordinating sensitive information integration and providing a support staff and appropriately cleared facilities for these functions pursuant to Deputy Secretary of Defense Memorandum (reference (w)).

3.12. Provide NII and CIO support to the mission of Information Operations in support of DoD Directive S-3600.1 (reference (l)).

3.13. Develop and oversee contingency and crisis response communications policies and planning for stabilization and reconstruction operations carried out by the Department with emphasis given to those executed in concert with the United States Government interagency process, to include the interaction of

DoD assets with foreign nations and nongovernmental organizations. Special emphasis shall be placed on migrating technologies uniquely suited to contingency operations that are often not used in DoD applications.

3.14. Participate, pursuant to the responsibilities and functions prescribed herein, in the DoD Planning, Programming, Budgeting, and Execution process, which includes proposing DoD programs, formulating budget estimates, recommending resource allocations and priorities, and monitoring the implementation of approved programs in order to ensure adherence to approved policy and planning guidance. This includes conducting program evaluation, assessments, and cross-program reviews, when applicable.

3.15. Address issues associated with meteorology, oceanography, and space weather programs (METOC) and provide overall guidance on DoD METOC matters. Ensure that DoD METOC systems and architectures are interoperable and consistent with GIG policies.

3.16. Address international issues associated with information and communications technologies, including technologies for the non-automatic movement, transmission, or reception of information. Negotiate and conclude international agreements relating to coalition command, control, and communications (C3) and IT policies, standards, and programs pursuant to DoD Directive 5530.3 (reference (n)). Exercise authority, direction, and control and approval of U.S. representation and negotiating positions in international fora and the conclusion of international agreements related to coalition C3 and international IT policies, standards, and programs.

3.17. Represent the Secretary of Defense at the North Atlantic Treaty Organization C3 Board.

3.18. Recommend changes to the Director, Program Analysis and Evaluation regarding to the content of the "virtual" Major Force Program for the GIG.

3.19. Serve on boards, committees, and other groups and represent the Secretary and Deputy Secretary of Defense on matters outside the Department pursuant to responsibilities and functions prescribed herein.

3.20. Periodically review assigned DoD Executive Agent responsibilities and functions to ensure conformance with DoD Directive 5101.1 (reference (x)).

3.21. Identify and convey enterprise-wide, information-related research requirements to the Director of Defense Research and Engineering (DDR&E) and other Senior Officials in the Department, as appropriate. In coordination

and consultation with the DDR&E, establish reliability, survivability, and endurability design criteria/standards for DoD C3 and develop and maintain a technology investment strategy to support the development, acquisition, and integration of DoD C3 services, systems, and processes.

3.22. Provide advice on issues related to all assigned responsibilities and functions to the Joint Requirements Oversight Council and Joint Capabilities Integration and Development System process.

3.23. Coordinate with the USD(I) to ensure that intelligence systems and architectures for collection, analysis, and dissemination of critical intelligence information follow net-centric strategies and are consistent and interoperable with DoD command, control, and communications and information-enterprise systems.

3.24. Coordinate with the Assistant Secretary of Defense for Homeland Defense to ensure interoperability of information systems with non-DoD organizations for homeland security and homeland defense.

3.25. Coordinate with the USD(AT&L) as the Vice Chair of the Defense Business Systems Management Committee to ensure that business systems and architectures for collection, analysis, and dissemination of militarily relevant information are consistent and interoperable with DoD command, control, communications, and information-enterprise systems.

3.26. Ensure that NII and CIO policies and programs are designed and managed in ways that improve standards of performance, economy, and efficiency and that all Defense Agencies and DoD Field Activities under the authority, direction, and control of the ASD(NII)/DoD CIO are attentive and responsive to the requirements of their organizational customers, internal and external to the Department.

3.27. Perform other such duties as the Secretary or Deputy Secretary of Defense may direct.

4. RELATIONSHIPS

4.1. In the performance of all assigned responsibilities and functions, the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer shall:

4.1.1. Report directly to the Secretary and Deputy Secretary of Defense.

4.1.2. Oversee and exercise authority, direction, and control over the Director, Defense Information Systems Agency.

4.1.3. In consultation and coordination with the USD(I), provide policy guidance to the Director, National Security Agency regarding network operations and IA matters.

4.1.4. Use existing facilities and services of the Department of Defense and other Federal Agencies, whenever practicable, to avoid duplication and achieve maximum efficiency and economy.

4.1.5. Provide advice to the OSD Principal Staff Assistants, as necessary, on DoD-wide issues associated with IRM, requirements analysis, budget-preparation matters, reporting activities, Congressional material, and enterprise architectural design related to those areas under the cognizance of the ASD(NII)/DoD CIO.

4.1.6. Serve as the sponsor of the Command, Control, Communications, and Intelligence Federally Funded Research and Development Center.

4.2. The Secretaries of the Military Departments shall provide timely advice to the ASD(NII)/DoD CIO and shall ensure that the policies and guidance issued by the ASD(NII)/DoD CIO are implemented in their respective Military Departments.

4.3. The Heads of the DoD Components shall coordinate with the ASD(NII)/DoD CIO on all matters relating to the responsibilities and functions cited in section 3, above.

5. AUTHORITIES

The ASD(NII)/DoD CIO is hereby delegated authority to:

5.1. Issue DoD Instructions, DoD publications, and one-time directive-type memoranda, consistent with DoD 5025.1-M (reference (y)), that implement policy approved by the Secretary or Deputy Secretary of Defense in the areas of assigned responsibilities and functions. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments, or their designees.

5.2. Obtain reports, information, advice, and assistance, consistent with DoD Directive 8910.1 (reference (z)) and DoD Directive 8000.1 (reference (aa)), as necessary, to carry out assigned functions.

5.3. Communicate directly with the Heads of the DoD Components. Communications with the Military Departments shall be transmitted through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary or Deputy Secretary of Defense in other DoD issuances, or except as provided in paragraph 5.4. below. Communications to the Commanders of the Combatant Commands, except in unusual circumstances, shall be transmitted through the Chairman of the Joint Chiefs of Staff. With the concurrence of the Chairman of the Joint Chiefs of Staff and the cognizant Combatant Commander, Chief Information Officers of the Combatant Commands may directly contact the ASD(NII)/DoD CIO or designee, when required.

5.4. Communicate directly with the CIOs of the DoD Components on all matters for which the ASD(NII)/DoD CIO is assigned responsibilities herein.

5.5. Establish arrangements for DoD participation in non-Defense governmental programs for which the ASD(NII)/DoD CIO is assigned primary responsibility.

5.6. Represent the Department of Defense and represent the Secretary and Deputy Secretary of Defense on matters prescribed herein with government agencies, representatives of the legislative branch, members of the public, and representatives of foreign governments and international organizations, as appropriate, in carrying out assigned responsibilities and functions.

5.7. Exercise the specific delegations of authority in enclosure 2.

6. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 2

E1. References, continued
E2. Delegations of Authority

E1. ENCLOSURE 1

REFERENCES, continued

(e) E-Government Act of 2002 (Public Law 107-347), December 17, 2002

(f) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992 (hereby canceled)

(g) Deputy Secretary of Defense Memorandum, "Establishment of the Deputy Under Secretary of Defense for Space Acquisition and Technology Programs," December 10, 1994 (hereby canceled)

(h) Deputy Secretary of Defense Memorandum, "Responsibilities and Functions of the Deputy Under Secretary of Defense for Space," March 8, 1995 (hereby canceled)

(i) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Pub. L. No. 104-106)," June 2, 1997 (hereby canceled)

(j) Chapter 113, Subchapter III of title 40, United States Code

(k) Executive Order 13011, "Federal Information Technology," July 16, 1996

(l) DoD Directive S-3600.1, "Information Operations," December 9, 1996

(m) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 9, 2002

(n) DoD Directive 5530.3, "International Agreements," June 11, 1987

(o) DoD Directive 4650.1, "Policy for Management and Use of the Electromagnetic Spectrum," June 8, 2004

(p) DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004

(q) Section 305 and Chapter 8, title 47, United States Code

(r) Part 300, title 47, Code of Federal Regulations (U.S. Department of Com-merce, National Telecommunications and Information Administration (NTIA), "Manual of Regulations and Procedures for Federal Radio Frequency Management)

(s) Secretary of Defense Memorandum, "Secretary of Defense Executive Agent for DoD Assets Supporting White House Military Office (WHMO)," February 17, 1999 (classified)

(t) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003

(u) DoD Directive 4650.5, "Positioning, Navigation, and Timing," June 2, 2003

(v) Executive Order 11161, "Relating to Certain Relationships Between the Department of Defense and the Federal Aviation Administration," July 7, 1964, as amended by Executive Order 11382

(w) Deputy Secretary of Defense Memorandum, October 10, 2003 (subject and content are classified)

(x) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002

(y) DoD 5025.1-M, "DoD Directives System Procedures," current edition

(z) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993

(aa) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002

Requests for copies can be forwarded to the Director, NII Administration and Management, Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, and will be provided based upon DoD policy and a need to know regarding classified information.

E2. <u>ENCLOSURE 2</u>

DELEGATIONS OF AUTHORITY

E2.1.1. Pursuant to the authority vested in the Secretary of Defense, and subject to the authority, direction, and control of the Secretary of Defense, and in accordance with DoD policies, Directives, and Instructions, the ASD(NII)/DoD CIO, or the person acting for the ASD(NII)/DoD CIO in his or her absence, is hereby delegated authority, as required, in the administration and operation of the Office of the ASD(NII)/DoD CIO to:

E2.1.1.1. Perform the duties and fulfill the responsibilities of the Secretary of Defense under sections 11312 and 11313 of title 40, United States Code. Assist the USD(Comptroller)/ DoD Chief Financial Officer in performing and fulfilling the responsibilities of the Secretary of Defense under section 11316 of title 40, United States Code.

E2.1.1.2. Make original security classification determinations (up to and including top secret) in accordance with E.O. 12958, "Classified National Security Information," April 17, 1995.

E2.1.1.3. Make written determinations for the conduct of all closed meetings of Federal Advisory Committees under the cognizance of the ASD(NII)/DoD CIO as prescribed by section 10(d) of the Federal Advisory Committee Act (5 U.S.C. Appendix II, 10(d)).

E2.1.2. The ASD(NII)/DoD CIO may redelegate these authorities, as appropriate, and in writing, except as otherwise specifically indicated above or prohibited by law, Directive, or regulation.

DoD Directive 8000.01

Management of the Department of Defense Information Enterprise

Date	February 10, 2009

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues and renames DoD Directive (DoDD) 8000.01 (Reference (a)), and assigns oversight responsibilities for DoD information management activities to the Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO), as the DoD CIO, consistent with DoDD 5144.1 (Reference (b)).

b. Implements sections 2223 and 2224 of title 10, United States Code (U.S.C.) (Reference (c)); Chapter 113 of title 40, U.S.C. (Reference (d)); Chapters 35 and 36 of title 44, U.S.C. (Reference (e)); and Office of Management and Budget Circular A-130 (Reference (f)) by establishing and reissuing policies for the management of the Department of Defense Information Enterprise.

c. Provides direction on creating an information advantage for DoD personnel and mission partners, and establishing and defining roles for CIOs at various levels within the Department of Defense consistent with References (c), (d), and (e).

d. Provides direction for information sharing among all DoD Components and with mission partners, consistent with the National Strategy for Information Sharing (Reference (g)).

e. Cancels DoDD 8100.01 (Reference (h)).

2. APPLICABILITY. This Directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Information shall be considered a strategic asset to the Department of Defense; it shall be appropriately secured, and shared, and made available throughout the

information life cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy.

b. Functional processes shall be simplified or otherwise redesigned to improve effectiveness and reduce cost before, or in conjunction with, making significant investments in information technology.

c. Each DoD Component shall have a CIO who reports directly to the Head of the Component. CIOs may also be designated at subordinate levels, but a reporting mechanism through the Component CIO must be maintained to ensure continuity of purpose.

d. Information solutions shall provide reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents consistent with Reference (e).

e. All aspects of the Department of Defense Information Enterprise, including the Global Information Grid (GIG) infrastructure and enterprise services and solutions, shall be planned, designed, developed, configured, acquired, managed, operated, and protected to achieve a net-centric environment, as envisioned in the National Defense Strategy of the United States of America (Reference (i)), capable of effectively and efficiently supporting the Department's outcome goals and priorities.

f. The DoD Enterprise Architecture, which is consistent with Reference (f) and composed of DoD enterprise and Component levels shall be maintained and applied to guide investment portfolio strategies and decisions, define capability and interoperability requirements, establish and enforce standards, guide security and information assurance requirements across the Department of Defense, and provide a sound basis for transition from the existing environment to the future.

g. Investments in information solutions shall be managed through a capital planning and investment control process that:

(1) Is performance- and results-based.

(2) Provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.

(3) Interfaces with the DoD key decision support systems for capability identification; planning, programming, budgeting, and execution; and acquisition.

(4) Requires the review of all information technology (IT) investments for compliance with architectures, IT standards, and related policy requirements.

h. Consistent with DoDD 5000.01 (Reference (j)) and DoDI 5000.02 (Reference (k)), acquisition strategies shall appropriately allocate risk between the Government and contractor; effectively use competition; tie contract payments to performance; and, where practicable, take maximum advantage of commercial off-the-shelf and non-developmental item technology. Information solutions shall be structured into useful segments that are as narrow in scope and brief in duration as practical; each segment shall solve a specific part of an overall mission problem and deliver a measurable net benefit independent of future segments.

i. Pilots, modeling and simulation, experimentation, and prototype projects shall be encouraged, especially when large, high-risk investments in information solutions are involved. However, these projects shall be appropriately sized to achieve desired objectives, and shall not be used in lieu of testing or acquisition processes to implement the production version of the information solution.

j. A well-trained core of highly qualified information management, information technology, and information assurance professionals shall be developed who can accept, anticipate, and generate the changes that the evolution of the Department of Defense Information Enterprise will enable in net-centric operations. The entire DoD workforce will similarly need to be trained and ready to take advantage of the Department of Defense Information Enterprise.

k. Disabled DoD employees or members of the public seeking information or services from the Department of Defense shall have access to and use of information and data comparable to the access and use by individuals who are not disabled, unless an undue burden would be imposed, to the extent required by section 794d of title 29, U.S.C. (Reference (l)).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Directive is effective immediately.

Gordon England
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities
Glossary

ENCLOSURE 1

REFERENCES

(a) DoDD 8000.01, "Management of DoD Information Resources and Information Technology," February 27, 2002 (hereby canceled)

(b) DoDD 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005

(c) Sections 2223 and 2224 of title 10, U.S.C.

(d) Sections 11101 and 11316, and Chapter 113 of title 40, U.S.C.

(e) Chapters 35 and 36 of title 44, U.S.C.

(f) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 28, 2000

(g) National Strategy for Information Sharing, October 2007[6]

(h) DoDD 8100.01, "Global Information Grid (GIG) Overarching Policy," September 19, 2002 (hereby canceled)

(i) The National Defense Strategy of the United States of America, September 2002[7]

(j) DoDD 5000.01, "The Defense Acquisition System," May 12, 2003

(k) DoDI 5000.02, "Operation of the Defense Acquisition System," December 8, 2008

(l) Section 794d of title 29, U.S.C. (Section 508 of the Rehabilitation Act of 1973, as amended)

[6] http://www.whitehouse.gov/nsc/infosharing/index.html
[7] http://www.whitehouse.gov/nsc/nss.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO, shall:

a. Lead the Department of Defense Information Enterprise:

(1) Exercise responsibilities as described in Reference (b).

(2) Serve as the DoD senior official for information resources management matters related to References (c), (d), (e), and (f).

(3) Report to and advise the Secretary and Deputy Secretary of Defense on the information resources implications of strategic planning decisions.

(4) Develop and maintain a strategic plan that describes how information resources management activities help accomplish the DoD mission, in accordance with Reference (e).

b. Provide standards for developing, maintaining, and implementing a DoD Enterprise Architecture. Establish mechanisms to ensure compliance with these standards.

c. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.

d. Ensure the integration and synchronization of the Department of Defense Information Enterprise activities.

e. Establish mechanisms to facilitate organizationally-tiered compliance reviews for all IT investments to ensure they comply with all enterprise architectures, IT standards and related policy requirements; and act as the oversight authority for IT compliance.

2. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). The USD(C)/CFO shall, pursuant to section 11316 of Reference (d) and in coordination with the ASD(NII)/DoD CIO and Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), establish policies and procedures to ensure that accounting, financial, and asset management systems and other related DoD information solutions are designed, developed, maintained, and used effectively to provide financial data reliably, consistently, and expeditiously, and support programmatic investment decisions.

3. HEADS OF THE OSD COMPONENTS AND CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Heads of the OSD Components and Chairman of the Joint Chiefs of Staff, according to their responsibility and authority for assigned functional areas, including supporting information resources, shall:

a. Improve DoD operations and procedures by ensuring the application of sound business practices and compliance with this Directive.

b. Exercise oversight for the evaluation and improvement of functional processes before making significant investments in information technology:

(1) Determine whether the function that IT will support is central to, or a priority for, the Department's mission.

(2) Determine whether the private sector or another Government agency can perform the function more effectively or at less cost.

(3) Outsource non-core and non-inherently Governmental functions to another Government agency or the private sector when it makes good business sense to do so.

(4) Benchmark functional area processes against models of excellence in other Government agencies or the private sector to develop, reengineer, simplify, or otherwise improve functional processes when the decision is made to retain the function in-house.

c. Participate in the OSD acquisition oversight process for major automated information systems and ensure functional leadership, management, and control of these systems throughout their life cycles.

d. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance, and interoperability.

4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. In addition to the responsibilities in paragraphs 3 and 5 of this enclosure, the Chairman of the Joint Chiefs of Staff shall appoint a Joint Community CIO.

5. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Appoint a DoD Component CIO who shall have core knowledge, skills, abilities, and experiences to carry out the requirements of References (c), (d), (e), and (f).

b. Clearly delineate the DoD Component CIO's role, responsibilities, and authority vis-à-vis those of the DoD Component Comptroller, the DoD Component Acquisition Executive or a similar position, functional area managers, and subordinate-level CIOs.

c. Take advantage of the opportunities that information management and IT can provide and ensure that the IT infrastructure will support enterprise, mission, functional, and Component strategies by positioning the DoD Component CIO to participate in that Component's strategic planning process.

d. Promote and forge a strong partnership among the Component's CIO and Comptroller, DoD Component Acquisition Executive or similar position, as well as other key senior managers and external mission partners when making and executing Component strategic decisions.

e. Designate, or authorize the designation of, subordinate-level CIOs, as needed, and ensure that the subordinate CIOs have a reporting mechanism through the Component CIO.

f. Ensure that the Component's IT investment portfolio aligns with the Department of Defense Information Enterprise policies and guidance, as required.

6. DoD COMPONENT CIOs. The DoD Component CIOs shall:

a. Have responsibilities and authorities as delegated in this Directive. Military Department CIOs shall have additional responsibilities as defined in Reference (c).

b. Head an office responsible for ensuring that the Component complies with, and promptly, efficiently, and effectively implements the policies and responsibilities in this Directive and the requirements of References (c), (d), (e), and (f).

c. Provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the Component according to References (c), (d), (e), and (f).

d. Participate in DoD CIO-led forums for governing the Department of Defense Information Enterprise.

e. Advise the DoD CIO and ensure that the policies and guidance issued by the DoD CIO are implemented; and contribute to the DoD strategic information resources management plan.

f. Establish programs to hire, train, and retain the information management, IT, and information assurance workforce consistent with this Directive.

g. Ensure information policy and functional requirements are reflected in architectures and plans across the DoD enterprise and Component levels as a means to ensure information sharing, visibility, assurance and interoperability.

h. Conduct organizationally-tiered reviews within their respective Components to ensure IT investments are in compliance with architectures at various levels, IT standards, and related policy requirements; and act as the Component's oversight authority for IT compliance.

GLOSSARY

Department of Defense Information Enterprise. The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems.

DoD enterprise-level. Relating to policy, guidance, or other overarching leadership provided by OSD Officials and the Chairman of the Joint Chiefs of Staff in exercising authority, direction, and control of their respective elements of the Department of Defense on behalf of the Secretary of Defense.

DoD Enterprise Architecture. A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment.

enterprise services. A common set of information resource capabilities designed to provide awareness of, access to, and delivery of information.

enterprise solution. The action of solving a problem or satisfying a requirement that affects the entire organization (e.g., Department of Defense).

GIG. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

information advantage. The superior position or condition derived from the ability to securely access, share, and collaborate via trusted information while exploiting or denying an adversary's ability to do the same.

information life cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

information technology. (A) Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use – (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

mission partners. Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

net-centric. Relating to or representing the attributes of a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared timely and seamlessly among users, applications, and platforms.

Web Sites

These are Internet addresses for direct access to the documents in this book.

U.S. Code materials are available at:

- U.S. House of Representatives, Office of the Law Revision Counsel: http://uscode.house.gov/lawrevisioncounsel.shtml
- GPO Access: http://www.gpoaccess.gov/uscode/index.html
- Cornell University Law School, Legal Information Institute: http://www4.law.cornell.edu/uscode/

44 U.S.C. 3501 et seq., "Paperwork Reduction Act"

40 U.S.C. Subtitle III, "Information Technology Management Reform Act"

10 U.S.C. Section 2223, "Information Technology: Additional Responsibilities of Chief Information Officers"

10 U.S.C. Section 2224, "Defense Information Assurance Program"

44 U.S.C. Chapter 36, 5 U.S.C. Chapter 37, and related titles, "E-Government Act"

OMB Circulars A-11 and A-130
http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc/
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

House of Representatives Documents
http://thomas.loc.gov/

H.R. Report 104-450
http://thomas.loc.gov/cgibin/cpquery/R?cp104:FLD010:@1(hr450)

DoD Directive 5144.01
http://www.dtic.mil/whs/directives/corres/pdf/514401p.pdf

DoD Directive 8000.01
http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf